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: NPS.gov
Bureau/Office: National Park Service / Information Resources
Date: 8/5/2019
Point of Contact:
Title: Chief, Web Services Division
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?

NPS.gov is the official National Park Service (NPS) website that delivers comprehensive information about NPS parks and programs to a global Internet audience. NPS.gov promotes transparency about NPS programs and services, improves communication and public outreach, and makes NPS resources, research, museum collections, and libraries easily accessible and widely available to the public. NPS Web authors within the Web Services Division develop and manage NPS.gov content using a content management system (CMS) that resides in a FedRamp certified private commercial cloud.

C. What is the legal authority?

- The Electronic Freedom of Information Act (FOIA) Amendments of 1996
- The Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995
- Presidential Memorandum on Transparency and Open Government, January 21, 2009
- OMB Open Government Directive, December 8, 2009
- OMB Circular A-130 – Managing Information as a Strategic Resource
- National Parks Omnibus Management Act of 1998, Section 104
- Executive order 13011 of July 16, 1996, "Federal Information Technology"
- Executive Order 12862 of September 11, 1993, "Setting Customer Service Standards"
- Executive Memorandum, "Expanding Access to Internet-based Educational Resources for Children, Teachers, and Parents," (April 18, 1997)

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* This privacy impact assessment analyzes the privacy implications for the official NPS.gov website.

E. Is this information system registered in CSAM?

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

UII Code: 010-000000554
System Security Plan (SSP) Name: NPS.gov SSP

☐ 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	

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)*
☒ No

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

☒ Yes: *Describe*
The survey presented by the CFI Group will use an adaptive PIA and is under OMB Control #1090-0007.
☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Email Address
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Name, email address and mailing/home address are collected in the "Contact Us" form used for visitors to submit comments/feedback, questions, and requests for brochures. Email address is the only required field. Information is not stored on the servers, but sent via email to the appropriate contact.

Name, mailing/home address, phone number, email address are collected from the "Lost and Found" form used to contact the visitor if the lost item is found and in case the staff have more questions. Information is not stored on the servers, but sent via email to the appropriate contact.

Some random visitors are selected to participate in a brief customer satisfaction survey to let the NPS know how NPS can improve their experience. This only information asked in the customer satisfaction survey is the age range of the visitor. The survey is designed to measure their entire experience at the conclusion of their visit. This survey is conducted

by an independent company CFI Group, on behalf of the NPS. NPS does not respond to any survey comments. To submit questions and comments, visitors must visit the Contact Us page of NPS.gov.

CMS content authors' full name, user principal name (UPN), and email are maintained as part of the authentication function of the CMS.

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

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*

CMS content authors are authentication through Active Directory Federated Services (ADFS) and full name, user principal name (UPN), and email are maintained as part of the authentication function of the CMS

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

Information collected from the public is used to improve NPS service or to respond to public requests. NPS does not share the public's information with any other outside organizations, except in unusual cases where it is required for authorized law enforcement purposes.

CMS content authors' information is used to grant access to the system to manage and deliver the content shown on the website (nps.gov), and it is also used to tie a content author to the content they created for version history user tracking.

Name, email address and mailing/home address are collected in the "Contact Us" form used for visitors to submit comments/feedback, questions, and requests for brochures. Email address is the only required field.

Name, mailing/home address, phone number, email address are collected from the "Lost and Found" form used to contact the visitor if the lost item is found and in case the staff have more questions.

Some random visitors are selected to participate in a brief customer satisfaction survey to let the NPS know how NPS can improve their experience. This survey asks for their age range. The survey is designed to measure their entire experience at the conclusion of their visit. This survey is conducted by an independent company The CFI Group, on behalf of the NPS. NPS does not respond to any survey comments. To submit questions and comments, visitors must visit the Contact Us page of NPS.gov.

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 may be provided to other NPS employees in order to provide customer service to the public.

☐ 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.*

NPS may share information with authorized law enforcement organizations for the conduct of investigations.

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

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

Contractors who provide system support will have access to data stored within the CMS.

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

NPS may share information with authorized concessioners in order to provide the service requested by individuals on our website.

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.*

NPS only collects information voluntarily provided by visitors to the NPS.gov who choose to communicate, interact, or request services from NPS. NPS uses that information to respond to the individual or provide the requested service. Any information that NPS collects may be subject to disclosure, but will be handled in accordance with the requirements of the Privacy Act and the Freedom of Information Act to ensure the greatest protection of personal privacy.

☐ 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.*

☒ Privacy Notice: *Describe each applicable format.*

A privacy notice is placed on the "Contact Us" and "Lost and Found" forms, which is linked from all NPS.gov webpages and may be found on the footer of each page. Below is the privacy notice.

"**IF YOU SEND US EMAIL**
You may choose to provide us with personal information, as in e-mail with a comment or question. We use the information to improve our service to you or to respond to your request. Sometimes we forward your e-mail to other government employees or authorized concessioners who may be better able to help you. Except for authorized law enforcement investigations, we do not share our e-mail with any other outside organizations."

Notice is also provided to individuals through the publication of this privacy impact assessment.

☒ Other: *Describe each applicable format.*

A Privacy Policy is posted on the NPS.gov website.

☐ None

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

Data is transmitted through email to the appropriate location, but not stored in NPS.gov.

I. Will reports be produced on individuals?

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

☒ No

Section 3. Attributes of System Data

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

Members of the public may choose to provide NPS with personal information, as in e-mail with a comment or question. NPS relies on the accuracy of the information provided by the individual. NPS CMS content authors' information are verified through Active Directory Federation Services (ADFS).

B. How will data be checked for completeness?

Members of the public may choose to provide NPS with personal information, as in e-mail with a comment or question. NPS relies on the completeness of the information provided by the individual. NPS CMS content authors' information are verified through Active Directory Federation Services (ADFS).

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

Members of the public may choose to provide NPS with personal information (e.g. contact information for a lost and found inquiry). NPS relies on the information provided by the individual to ensure that the data is current. NPS CMS content authors' information are verified through Active Directory Federation Services (ADFS).

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

Record retention schedule for NPS.gov is N1-79-08-8, Information and Public Image Management Records, Item A.1. The disposition is permanent. Transfer permanent special media, and electronic records along with any finding aids or descriptive information (including linkage to the original file) and related documentation by calendar year to the National Archives and Records Administration (NARA) when 3 years old. Digital records will be transferred according to standards applicable at the time.

Transfer all other permanent records to NARA 15 years after closure. Non-permanent Information and Public Image are destroy/delete records 15 years after closure.

Records retention schedules indicating retention periods for information collected from members of the public through NPS.gov and directed to specific park/office are located and maintained at the NPS location responsible for use, retention, processing, disclosure and destruction of the information.

Lost and found records are covered under N1-79-08-2, Item 2. These are temporary records and 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?

Procedures for disposition of the data at the end of the retention period for information collected from members of the public through NPS.gov and directed to specific park/office are located and maintained at the NPS location responsible for the use, retention, processing, disclosure and destruction of the information.

CMS history data is regularly backed up and stored on the Amazon Web Services (AWS) long term cloud storage.

Approved disposition methods for 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.

Privacy risks are well mitigated and risk to individuals is minimal. Public PII is not stored on any of the NPS.gov servers, but is sent via NPS email to the appropriate group (park, program, etc.). The NPS.gov CMS and its computer infrastructure employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

NPS.gov uses HTTPS to ensure all communications between NPS.gov and members of the public are encrypted and secure, and to protect the privacy and integrity of any exchange of information. Encryption prevents the public information from being read or changed while in transit as well as interception or alteration, which can subject users to eavesdropping, tracking, and the modification of received data.

NPS.gov is rated at the FISMA Moderate level. The system is housed on Amazon Web Services, a secured FedRAMP certified private cloud environment that houses the CMS and content delivery network operated by Akamai. The CMS by which the website is published is accessed by NPS content authors using Active Directory Federation Services for authentication. Direct connection for administrators is done using a secured FIPS compliant virtual private network (VPN).

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Only those authorized employees and contractors who have a need for access will have access to the system using least privilege principles. Personnel authorized to access the system must complete all Security, Privacy, and Records management training and sign the Rules of Behavior.

Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

Virus protection measures are used on the computer systems and the software is regularly updated. These are computer security measure that, in addition to maintaining our computer systems, also ensures that all files that we develop and/or post on our web servers are virus-free. When a user requests a file for download from this site, it is possible, though unlikely, that the data may contract a virus and become corrupted before it reaches the user's computer. The Department of the Interior is not responsible for files that may become corrupted as the data travels the Internet.

Amazon Web Services (AWS) uses AWS CloudTrail. Information is collected on administrator / user access to the AWS virtual machine. CloudTrail records AWS application programming interface (API) calls, information includes: the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.

NPS.gov uses session cookies for technical purposes such as to enable better navigation through the site, or to allow you to customize your preferences for interacting with the site. Like many websites, nps.gov uses "persistent cookie" technology. A persistent cookie is a small text file that this website places on your web browser so that it can gather anonymous summary demographic information, and remember your browser when it is used to visit our site again later—kind of like cookie crumbs! (Hence the name.)

These cookies uniquely identify a browser on a computer, but never a person. In other words, if the same person uses Chrome and Internet Explorer, two unique browser cookies will be assigned, one for each browser, so that person will be counted as two different visitors because visits are based on browsers, not computers or persons.

These persistent cookies fall under the category of "Tier 2 – multi-session without PII" as described by the Office of Management and Budget (OMB) Memorandum "Guidance on Online Use of Web Measurement and Customization Technologies", dated, June 25, 2010. This tier encompasses any use of multisession web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of such technologies).

NPS.gov provides a link for users to "opt-out" and disable cookies in their browsers. Click here to "opt-out" and disable cookies in the browser

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*

Information collected from the public is used to improve NPS service or to respond to public requests. NPS.gov delivers comprehensive information about National Park Service (NPS) parks and programs to a global Internet audience and makes NPS resources, research, museum collections, and libraries easily accessible to the public. CMS content author information is necessary to develop and manage NPS.gov content.

☐ 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?

NPS.gov does not derive new data or create previously unavailable data about an individual through data aggregation.

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?

Users are visitors to the website have public read access to content published on NPS.gov. Contractors/Developers have access to view the database and all areas of the code. These workers all have background checks and login with their Personal Identity Verification (PIV) card. These workers do not have access to the servers themselves. System Administrators have access to view the database and all areas of the code. These workers all have background checks and login with their PIV card. In addition, these administrators have access to the servers (through PIV authentication).

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?*

The NPS.gov contract has the appropriate Privacy Act contract clauses, below, including, information collected for tracking and customization (cookies), information stored automatically about the user, how emailed information is used, and information regarding links to other sites.

52.224-1 Privacy Act Notification (Apr 1984)
52.224-2 Privacy Act (Apr 1984)

☐ 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*

☒ No

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

NPS.gov uses persistent cookies to enhance visitor's experience on nps.gov while also protecting their privacy. These cookies uniquely identify a browser on a computer, but never a person. These persistent cookies fall under the category of "Tier 2 – multi-session without PII" as described by the Office of Management and Budget (OMB) Memorandum "Guidance on Online Use of Web Measurement and Customization Technologies", dated, June 25, 2010. This tier encompasses any use of multisession web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of such technologies).

NPS.gov uses persistent cookies:

- To remember the user when a user comes back to the site, to avoid having to invite users to take the customer satisfaction survey or receive a newsletter every time the same user visits the website.

- To get aggregate metrics on site usage to understand how people are using the site and how we can make it better. We use web metrics services to track activity on nps.gov. Government agencies only ever receive traffic statistics anonymously and in the aggregate.

- To gather anonymous summary demographic information about our visitors such as gender, age range and areas of interest for adults over the age of 18. This demographic information is used to help us better understand our visitors' interests and needs to more effectively develop content to serve you.

NPS.gov provides a link for users to "opt-out" and disable cookies in their browsers.
Click here to "opt-out" and disable cookies in the browser

CMS maintains audit, system and user's logs on all the activities performed by the system content authors such as their username, last login, and content updated.

M. What controls will be used to prevent unauthorized monitoring

Members from the public have read-only access to the nps.gov site. CMS administrators' system access is limited to personnel who have a need to know of the information for the performance of their official duties. The number of administrative users is limited, using least privilege principle.

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*

(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*

(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 NPS.gov Information System Owner is the official with ultimate responsibility for implementing adequate controls and protecting the privacy rights of individuals affected by the use of the system and interactions on the NPS.gov website.

The Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with the Federal laws, regulations and policies for the data collected, used and managed, and for making decisions on privacy issues, in consultation with the NPS 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 Information System Owner has responsibility for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner.

The NPS Privacy Officer is responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the DOI Privacy Office.