



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 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: Volunteer.gov System Decommissioning

Date: March 15, 2022

Bureau/Office: National Park Service

Point of Contact

Name: Felix Uribe

Title: NPS Associate Privacy Officer (APO)

Email: nps_privacy@nps.gov

Phone: (202) 354-6925

Address: 12201 Sunrise Valley Drive, MS 242, 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

B. What is the purpose of the system?

The purpose of the Volunteer.gov system was to serve as a one-stop recruitment resource for public citizens to explore and apply for volunteer and public service projects to support the mission of federal agencies in the areas of, but not limited to, conservation, restoration,



construction, or rehabilitation of natural, cultural, historic, archaeological, recreational, or scenic resources.

The legacy Volunteer.gov website supported citizen volunteerism and service-learning opportunities for youth and adults. The system enabled recruitment, application, selection, and reporting of program participants and project activities. The application supported a multi-agency partnership and allowed public land management agencies (U.S. Department of the Interior (DOI), U.S. Forest Service, Natural Resources Conservation Service, and the U.S. Army Corps of Engineers) to collect applications and report on progress in meeting strategic goals of expanding and providing volunteer and service-learning opportunities to citizens. The National Park Service (NPS) was the lead agency responsible for implementation and maintenance of the system.

The legacy Volunteer.gov system has been replaced by the Stewardship Engagement Platform (SEP) which has been assessed and documented under [Stewardship Engagement Platform PIA](#).

The assets of the Volunteer.gov system have been disposed in the following manner:

Software: The Volunteer.gov software ran on virtual machines hosted in the DOI Data Center. All virtual machines that comprised the system were decommissioned by the DOI Data Center.

Hardware: Hardware and peripherals were decommissioned and sanitized in accordance with DOI sanitization procedures.

Data: In production, the transactional data in the Volunteer.gov system was hosted in a SQL Server database in the DOI Data Center. Server hard drives remained within the DOI Data Center organizational control until destroyed on site. Storage devices were excessed, and drives shredded in accordance with DOI policy or will receive sanitization, verification, and certification services. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

Documentation: System and project documentation was archived and is now stored for reference with the file image. This project documentation does not contain PII.

C. What is the legal authority?

16 U.S.C. §460l; Outdoor Recreation Authority, Public Law 92-300; Volunteers in the National Forest Act of 1972, 16 USC 558 a-d; Volunteers in the National Forests Program, 16 USC 583j-4; Forest Foundation Volunteers, 16 USC 1246; Administration and development of national trails system, 16 USC 1250; Volunteer trails assistance, 31 USC 3325; Authorizes payment of vouchers, 16 U.S.C. § 1g; Agreements for the Transfer of Appropriated Funds to Carry Out NPS Programs, 16 U.S.C. § 1246(h)(1); Agreements to Operate, Develop, and Maintain Portions of National Trails, 16 U.S.C. § 1a-2(j)); Agreements Concerning Cooperative Research and Training on NPS Resources, 38 USC §4301; The Uniformed Services Employment and



Reemployment Rights Act, Presidential Memorandum; Expanding National Service, July 15, 2013, and Department of the Interior Secretary Order No: 3332.

D. Why is this PIA being completed or modified?

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

E. Is this information system registered in CSAM?

- Yes

UII: 010-000000709; Volunteer.gov System Security and Privacy Plan

- 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.
NA	NA	NA	NA

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

- Yes:

- INTERIOR/DOI-05, Interior Volunteer Services File System, May 23, 2001 66 FR 28536); modification published September 7, 2021 (86 FR 50156)
- INTERIOR/DOI-58, Employee Administrative Records, April 20, 1999 (64 FR 19384); modification published February 13, 2008 (73 FR 8342) and September 7, 2021 (86 FR 50156)
- OPM/GOVT-1, General Personnel Records, December 11, 2012 (77 FR 73694); modification published November 30, 2015 (80 FR 74815)
- OPM/GOVT-5, Recruiting, Examining, and Placement Records, March 26, 2014 79 FR 16834); modification published November 30, 2015 (80 FR 74815) and December 1, 2021 (86 FR 68291)
- INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/ EACS), March 12, 2007 72 FR 11040 ; modification published September 7, 2021 (86 FR 50156)

These SORNs may be viewed on the DOI SORN website at <https://www.doi.gov/privacy/sorn>.



No

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

Yes:

- OMB 1093-0006, Natural and Cultural Resource Agencies Customer Relationship Management; Expiration Date: October 31, 2024
- OMB 0596-0080, Volunteer Service Application for Natural and Cultural Resources; Expiration Date: October 25, 2021

No

Section 2. Summary of System Data

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

Other: The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

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.

Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

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



- Paper Format
- Email
- Face-to-Face Contact
- Website
- Fax
- Telephone Interview
- Information Shared Between Systems
- Other: Describe.

Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

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

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

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

- Within the Bureau/Office

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

- Other Bureaus/Offices

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

- Other Federal Agencies

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.



Tribal, State or Local Agencies

Contractor

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

No

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were exsessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

I. Will reports be produced on individuals?



Yes

No

Section 3. Attributes of System Data

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

Not Applicable. The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

B. How will data be checked for completeness?

Not Applicable. The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

Not Applicable. The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

Volunteer.gov system records are maintained in accordance with the National Park Service Records Schedule, Partnerships (Item 7), which has been approved by the National Archives and Records Administration (Job No. NI-79-08-6). The record retention schedule for short-term interpretation and education program records data is temporary, which requires destruction/deletion of records 7 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 Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. Approved disposition methods include degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

Server hard drives remained within the DOI Data Center organizational control until destroyed on site. Storage devices were excessed, and drives shredded in accordance with DOI policy or will receive sanitization, verification, and certification services. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

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.

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

There is a limited privacy risk for the decommissioning of the Volunteer.gov system infrastructure related to potential unauthorized access or mishandling of the residual data that remains in the Volunteer.gov system before it can be destroyed. NPS implemented physical, administrative, and logical controls to protect the image file until final disposal.

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

No

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

Yes

No

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

Yes

No



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

Yes

No

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

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

F. Are the data or the processes being consolidated?

Yes, data is being consolidated.

Yes, processes are 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

Contractors

Developers

System Administrator

Other:

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. Only authorized NPS personnel had access to the equipment and residual data pending final destruction.

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

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. Only authorized NPS personnel had access to the equipment and residual data pending final destruction.



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.

Privacy Act contract clauses were included in the contract. In addition, all contractors with access to the system and/or data were required to have full NPS background investigations, NPS credentials, PIV cards, and government-furnished equipment (including data-at-rest pre-boot authentication) used to access the system.

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

No

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

Yes

No

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

Not Applicable. The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

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

Not Applicable. The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until



destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period.

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.

The Volunteer.gov system has been decommissioned. PII is no longer being collected or hosted in this legacy environment. All data in the Volunteer.gov system hosted in a SQL server database within DOI Data Center was secured in the organizational control until destroyed on site. All Storage devices were excessed, and drives shredded in accordance with DOI policy. A file image of the virtual machine is stored in a secure, system administrator access only repository managed by NPS Information Resources and will be destroyed at the expiration of the records retention period. The decommissioning plan provides details on the disposal of the information technology resources. There are physical controls in place to protect data that was migrated or still being maintained in other DOI systems as marked above.

(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*

The decommissioning plan provides details on the disposal of the information technology resources. There are technical controls in place to protect data that was migrated or still being maintained in other DOI systems as marked above.

(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*

The decommissioning plan provides details on the disposal of the information technology resources. There are administrative controls in place to protect data that was migrated or still being maintained in other DOI systems as marked above.

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 Chief of Resource Information Services Division, National Information Service Center is the Information System Owner. The Volunteer.gov Information System Security Officer manages the security controls in the system. These officials are responsible for ensuring appropriate security and privacy controls are implemented and managed in accordance with Federal and DOI policy. The NPS Associate Privacy Officer is responsible for addressing any privacy related complaints.

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 System Owner and Information System Security Officer are responsible for managing the security and privacy controls in the system and ensuring proper use of the system and data. These officials and the NPS Associate Privacy Officer are responsible for reporting any loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information to DOI-CIRC, DOI's incident reporting portal.