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: Stewardship Engagement Platform (SEP)
Bureau/Office: National Park Service, Information Resources Management
Date: 6/9/2020
Point of Contact:
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: 202-354-6925
Address: 12201 Sunrise Valley Drive, Reston VA 20192

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Stewardship Engagement Portal (SEP) is 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.

SEP supports citizen volunteerism and service learning opportunities for youth and adults. The system also provides for management processes that enable recruitment, application, selection, and reporting of program participants and project activities. The platform is designed and developed through a multi-agency partnership and allows public land management agencies (U.S. Department of the Interior (DOI), U.S. Forest Service, Natural Resources Conservation Service, U.S. Army Corps of Engineers, and The National Arboretum) to securely collect applications, agreements, and report on progress in meeting strategic goals of expanding and providing volunteer and service learning opportunities to citizens. The National Park Service (NPS) is the lead agency responsible for implementation and maintenance of the system. Salesforce is the cloud platform provider for the SEP portal.

Volunteers will access the system from the public facing Volunteer.gov Community portal (https://volunteer.gov) which will be discoverable by internet search. Members of the public may browse volunteer opportunities without creating a user account. Prospective volunteers may create an account and submit on-line applications for desired opportunities. Volunteers can then maintain their profile, view the status and history of their applications, withdraw an application, and establish criteria for recommendations for volunteer opportunities.

Volunteer coordinators, youth stewardship coordinators, and other government agency staff, contractors, and partners will access the system through a separate, non-public facing portal. This portal will provide access to system functions enabling creation and publication of volunteer and youth stewardship opportunities content information for posting and display on the public facing community website.

The Salesforce mobile application is included with the Salesforce platform licensing and is available for devices running Apple and Android operating systems through the applicable app store. Use of the SEP mobile application is limited to authorized personnel of DOI and its partners. Once the user logs on to the mobile app, they are automatically connected to the production environment using industry-standard protocols. The Salesforce platform provides configuration options for managing authentication and access for mobile devices.

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
- Department of the Interior Secretary Order No: 3332
- 21st Century Conservation Service Corps Act, March 12, 2019

D. Why is this PIA being completed or modified?

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

E. Is this information system registered in CSAM?

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

☒ Yes: UII 010-000000709 Stewardship Engagement Platform 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.*
Volunteer.gov	Volunteer recruitment, position and event posting, and management	Yes	All items identified in Section 2.A. for purpose of identification, application and selection of individuals for volunteer positions or events.
NPS Volunteers in Parks Reporting Module	Aggregated volunteer utilization reporting	No	

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

☒ Yes:

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

☐ 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, 11/30/2021
- OMB 0596-0080, Volunteer Service Application for Natural and Cultural Resources, 10/31/2021

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Disability Information
☒ Child or Dependent Information
☒ Employment Information
☒ Education Information
☒ Emergency Contact
☒ Race/Ethnicity
☒ Military Status/Service
☒ Mailing/Home Address
☒ Home Telephone Number
☒ Medical Information
☒ Personal Email Address
☒ Security Clearance
☒ Personal Cell Telephone Number
☒ Other: *Specify the PII collected.*
In general, the PII collected is information typically used to determine if an individual meets the requirements for participating in an event or holding a volunteer position (e.g. data typical of an employment application). In addition to the PII fields identified above, the following data is collected:

- Name: Salutation, First Name, Middle Name, Last Name, Suffix
- Age (calculated from the date of birth)
- Phone/Mobile Number
- Address: Street, City, State/Territory, Country, Zip/Postal Code
- Military Status
- National Service Status
- Disability (Yes/No only)

- Citizenship: Country of Citizenship, Verification Status, Type of Visa
- Languages Spoken
- Skills
- Certifications
- Education: Institution Attended, Level Achieved, Year Received, Field of Study/Major
- Volunteer and Work Experience
- References: Name, Relationship, Phone, Email
- Photo Release
- Emergency Contact: Name, Relationship, Phone, Email
- Parent/Guardian: Name, Address, Phone, Email
- States of Interest
- Categories of Interest
- Demographic information (e.g. ethnicity, race) will be used for statistical reporting purposes for government mandated or program performance reporting.
- Username and/or email address and password collected from individuals who have a volunteer or government user account. A PIN may be issued for use of a mobile device.

Record IDs are assigned to object records such as case, applicant, opportunity identifiers or other unique record IDs. These are not all inherently PII but certain record IDs may be linked to an individual. These record IDs are necessary for system and data management functions.

Internet Protocol (IP) addresses are collected for security purposes and allows IP restrictions to be applied and supports incident response.

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
☐ Telephone Interview
☐ Information Shared Between Systems
☒ Other: Mobile application

Mobile capability is part of the platform. Authorized government users with non-privileged accounts can download a mobile application from the applicable online store and pair it to their account. Government users who are system administrators or who have privileged accounts are prohibited from using the mobile application when using their privileged accounts. The SEP mobile application is not enabled for the general public.

Face-to-face contact is performed by Federal employees registering individuals in person at volunteer events. The information is gathered by paper and some information may be later entered into the system. Furthermore, all volunteers must sign paper volunteer agreement once accepted for a volunteer position.

Information will be collected from the public-facing Volunteer.gov Community portal. Prospective volunteers may create an account and submit on-line applications for desired opportunities. Volunteers can then maintain their profile, view the status and history of their applications, withdraw an application, and establish criteria for recommendations for volunteer opportunities.

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

The PII collected is used by DOI and participating public land management agencies to identify persons interested in participating in a government volunteer program, and for all necessary purposes for managing the volunteer program.

PII collected will be used to support the citizen engagement and management processes that enable recruitment, application, selection, and reporting of citizen engagement opportunities and project activities. PII will be used to authenticate individuals to the system, to enable communications between individuals and personnel, contractors, and partners of the participating agencies, and to enable submission of applications and resumes, record participation and timesheets, determine participant award eligibility, and generate performance and analytical reports. Information is collected to authorize placement and management of youth and adults for performing service on public lands. The information is used to provide citizens engaged in projects appropriate and safe placement and to ensure those eligible participants are covered by workman's compensation and other benefits as defined under legal, regulatory and policy standards and guidelines.

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.*

SEP will be used across all NPS parks, programs and offices to execute citizen engagement and management processes that enable recruitment, application, selection, and reporting of youth and adults service learning and project activities. Data sharing will be restricted within the Bureau based on the user's role and permission and park, program or office assignment.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

SEP will be used across DOI Bureaus and Offices to execute citizen engagement and management processes that enable recruitment, application, selection, and reporting of volunteers and volunteer activities. Data sharing will be restricted between and within the DOI Bureaus based on the user's role and permission and organizational assignment.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

SEP will be used by non-DOI agencies to execute service learning and volunteer engagement management processes that enable recruitment, application, selection, and reporting of youth and adults engaged in stewardship activities and projects and as required by law in accordance with the routine uses outlined in DOI-05, Interior Volunteer Services File System. Data sharing will be restricted between and within the agencies based on the user's role and permission and organizational assignment. Currently, the non-DOI agencies include the U.S. Army Corp of Engineers and the Department of Agriculture, however other agencies are showing interest in joining so as that occurs, this list will be expanded.

☐ 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 are responsible for the operations and maintenance of the software platform. Contractors need access to the platform to provide support and maintenance for the application that host PII but will not have access to the actual PII data. This maintenance is critical to protecting the system and the PII contained within the system. Salesforce, the cloud platform provider maintains a Federal Risk and Authorization Management Program (FedRAMP) authorization and undergoes a security assessment by a third party assessment organization each year.

NPS may contract with other commercial organizations to provide application development and configuration and operations and maintenance of the software platform or specific applications. Contractor staff will be required to undergo background checks as defined by NPS policy and procedures. Contractor staff access will be restricted to data on a need to know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the System Security Plan and Privacy Plan.

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

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.*

Individuals voluntarily provide information when creating a profile or contact in the system, submitting applications and agreements, and submitting timesheets, reports and correspondence. Users will be provided a Privacy Act Statement at the time of registration and will be offered the opportunity to accept or decline to provide information; however, declining to provide information may impact the ability of NPS to communicate with an individual and may impact an individual's ability to effectively communicate their interest in or compete for volunteer positions or events and record participation for award eligibility or workman's compensation if needed or emergency occurs.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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

☒ Privacy Act Statement: *Describe each applicable format.*

A link to a DOI Privacy Act Statement is provided when collecting PII on every screen and at log in to the system.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and the applicable published SORNs.

☒ Other: *Describe each applicable format.*

Users are provided with a privacy and security warning banner when accessing the system.

☐ None

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

Information in the system may be retrieved by Name, Phone number, Email address, or userid.

I. Will reports be produced on individuals?

☒ Yes:

In general, reports are only generated by agencies on aggregated statistical information. Individual volunteers may generate a report of their volunteer work history.

☐ No

Section 3. Attributes of System Data

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

Where possible, PII information is collected directly from the individual who will have access to verify and update the data to ensure accuracy, relevance, and completeness. To the extent practicable, data entry validations will be implemented to ensure data integrity. Federal agency staff during the course of the application and user management processes may periodically verify that the information provided is accurate and complete and may request the individual update or correct pertinent data.

Volunteer coordinators review applications for disposition, interview candidates for positions, and provide an agreement for acceptance by the volunteer. Volunteer coordinators may verify information during the disposition, interview or agreement processes and may advise the volunteer to update information in SEP. Volunteer coordinators will not have access to make changes to the volunteer's profile information.

B. How will data be checked for completeness?

To the extent practicable, data entry validations will be implemented to ensure data integrity. Federal agency staff during the course of the application and user management processes may periodically verify information provided is accurate and complete.

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

All applications, agreements and reporting will be actively managed until close out of the respective processes. Individuals may periodically be prompted to update their information by Federal agency staff or when accessing the system to explore stewardship engagement opportunities.

Inactive records may be removed from the system in accordance with records retention policies and procedures.

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

Records retention depends on the type of partnerships and application/agreements for citizens engaging in stewardship engagement programs, the approved records retention schedule and the needs of the agency.

SEP records related to collaboration with individuals; organizations; tribal, state, and local governments; and other Federal agencies to enhance and supplement NPS resources and activities 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. Nl-79-08-6). These records may include establishing and managing projects and programs in partnerships with others that span all NPS functions, interpretive and educational partnerships, Volunteers in Parks programs, cooperating associations, donations, and fundraising. The disposition for short-term interpretation and education program records is temporary and records are destroy/delete 7 years after closure. The disposition for routine interpretation and education records is temporary and records are destroyed/deleted 3 years after closure.

SEP records related to interpretive and educational programs for park visitors developed by park, regional, and headquarters staff are maintained in accordance with the National Park Service Records Schedule Interpretation and Education (Item 6), which has been approved by the National Archives and Records Administration (Job No. Nl-79-08-5). The disposition for short-term interpretation and education program records is temporary and records are destroy/delete 15 years after closure. The disposition for routine interpretation and education records is temporary and records are destroyed/deleted 3 years after closure.

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

For temporary records, approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and the 384 Departmental Manual 1. Detailed disposition procedures will be defined and published on the internal site for SEP administrative procedures.

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 are privacy risks related to hosting, processing and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which will be referenced in the System Security and Privacy Plan. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information. Volunteer profiles are accessible via user id and password to the individual, and the individual will be able to make edits to their information as needed. A very limited number of system administrators may have limited access to volunteer profiles for support purposes only (e.g. password reset, login monitoring, incident response, etc.).

There is a risk that individuals may not know why their information is being collected, how it will be used or who it will be shared with during and following the application, partnership, and reporting processes. System users who may submit PII will be provided a link to the Privacy Act statement and is also available upon request. The public is also provided notice of the collection, uses and sharing of information through this PIA and the applicable system of records notices.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Access to administrative functions is strictly controlled. System administrators periodically review audit logs to prevent unauthorized monitoring. Users are required to accept rules of behavior when using the system. All users must have an account in the system and user authentication protocols are enforced based on the user's role and permissions, i.e. personal identity verification (PIV) cards, two factor authentication, two step verification. Government employees, contractors, and partners (collectively, Government Users) will be required to use two factor authentication. Government Users will be authorized for their role and permissions using a formal process for ensuring least privilege access is maintained before their accounts are created in SEP. Government Users will authenticate to SEP using the applicable agency identity provider (e.g. Active Directory Federated Services for DOI) and their GSAccess issued PIV card. Government Users (except system

administrators) may use the Salesforce Authenticator application for two-factor authentication on their mobile device after users connect an authenticator application or register a security key with their Salesforce account. The Salesforce Authenticator mobile application sends a push notification to the user's mobile device when the Salesforce account requires identity verification. The user responds on the mobile device to verify or block the activity. Salesforce Authenticator also generates verification codes, sometimes called "time-based one-time passwords" (TOTPs). Users can choose to enter a password plus the code instead of responding to a push notification from the application for two-factor verification.

In addition, Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Session cookies are used to record encrypted authentication information for the duration of a specific session, but do not include username, password or other PII. Platform encryption has been deployed to encrypt data at rest. Other security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk that PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes or use of data. Federal employees and contractors are required to take annual mandated security, privacy and records management as well as role-based training where applicable and sign the DOI Rules of Behavior prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is risk that erroneous information may be collected. This risk is mitigated by allowing individuals to access and update their records in the system.

There is a risk that information in the system will be maintained longer than necessary to achieve the agency's mission. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

There may be a risk associated with hosting the system with a cloud service provider. SEP is hosted in the Salesforce Government Cloud that is FedRAMP authorized. The Salesforce Government Cloud is a partitioned instance on the platform as a service (PaaS) and software as a service (SaaS). It is a multi-tenant community cloud infrastructure specifically for use by U.S. Federal, state, and local government customers, U.S. government contractors, and federally funded research and development centers

Salesforce maintains FedRAMP authorization and undergoes a security assessment by a third party assessment organization each year.

There is a risk of data leakage or compromise of the mobile application. SEP system administrators control mobile application functions through configuration of connected applications policies on the Salesforce platform. Connected application policies enable control of mobile session timeouts, PIN code enforcement, and other restrictions on mobile applications in addition to other platform level controls on permissions, authentication, and encryption. The mobile application runs in a sandbox which restricts and isolates the application from other applications to prevent unauthorized data sharing.

Government users must use an authorized mobile device that is registered to the Agency mobile device manager, which allows the Agency to disable the device or delete device content in the event of loss, theft, or other suspected incident or compromise. The mobile application uses an industry-standard protocol to establish a secure connection to the platform with each session without exposing user passwords. Passwords are not stored on the mobile device. The mobile application is not enabled for the general public.

There is a risk of identifying user location from use of the mobile application and mobile devices. This risk is mitigated through controls enabled on the SEP platform. These controls are managed and monitored under change management procedures to ensure only authorized changes are enabled by authorized personnel. IP addresses are collected for security purposes to manage IP address restrictions and respond to incidents. However, IP addresses are not used to monitor and track specific individuals or their location data.

Salesforce support personnel require access to the platform to provide support and maintenance, but will not have access to the data and PII. This maintenance is critical to protecting the system and any PII contained in the system. A formal Assessment and Authorization for issuance of an authority to operate will be/has been conducted in accordance with the Federal Information Security Modernization Act (FISMA), and the system has been rated as moderate, requiring management, operational, and technical controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. As part of continuous monitoring, continual auditing will occur to identify and respond to potential impacts to PII information.

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:

Federal agencies are provided authority to maintain and collect youth and adult applications and agreements for citizens interested or performing stewardship projects in support of agency's mission. Information on individuals applying for and participating in stewardship engagement and volunteer positions and events are necessary for enabling competitive selection of applicants, effective assignment of individuals to shifts, locations, and roles, determining individual award eligibility, and ensuring management of workers compensation and other legal and regulatory requirements.

☐ 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?

New data is not created or derived by the system.

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 - volunteers and Volunteer Coordinators
☒ 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?

Access will be restricted for all users. Each user will be assigned a role (functions) and permissions. The role will determine what function the user may execute in the system while the permissions will define what records the user can create, read, edit or delete. For example, a park unit volunteer coordinator will have access only to the volunteer applications for positions and events for the park units for which they are responsible.

Select PII data fields will be encrypted and only available on a need to know basis. For example, certain demographic information such as ethnicity will be viewable by the individual and not by other users. This type of data may be used for analytical and performance reporting on an agency, bureau or unit and is not necessary for viewing on the individual level.

System management staff may on occasion be required to view PII in the performance of their duties for troubleshooting or system maintenance purposes. Employee or contractor staff with privileged accounts will be subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity.

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?*

Contractors are responsible for designing, developing and maintaining the system, and in accordance with DOI policies, Privacy Act contract clauses are included in all contractor agreements in accordance with and subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations.

Contractor employees interfacing with the system and/or related data or providing services, administration or management are required to sign nondisclosure agreements as a contingent part of their employment. Contractor employees are also required to sign the DOI's Rules of Behavior and complete security and privacy training prior to accessing a DOI computer system or network. Information security and role-based security training must be completed on an annual basis as an employment requirement. Contractor and/or contractor personnel are prohibited from divulging or releasing data or information developed or obtained in performance of their services, until made public by the Government, except to authorized Government personnel. Contractors are also subject to Federal Acquisitions Regulations (FAR) with regard to sensitive data, including:

- FAR Subpart 4.19 - Basic Safeguarding of Covered Contractor Information Systems
  - FAR Clause 52.204-21
- FAR Subpart 24.1 - Protection of Individual Privacy Contracts involving design, development, or operation of systems of records subject to the Privacy Act of 1974
  - FAR Clause 52.224-1 "Privacy Act Notification"
  - FAR Clause 52.224-2 "Privacy Act"
- FAR 39.101-Acquisition of Information Technology-General-Policy in acquiring IT, agencies must identify their requirements pursuant to, A-130, including consideration of privacy and security, and shall include appropriate IT security policies and requirements, including the use of NIST common security configurations.
- FAR 39.105-Acquisition of Information Technology-General-Privacy - IT contracts must address privacy in accordance with the Privacy Act of 1974 and FAR Part 24, including rules of conduct, anticipated threats and hazards, safeguards, and Government inspection
  - FAR Clause 52.239-1 "Privacy or Security Safeguards"
- FAR Subpart 27.4-Rights in Data and Copyrights - Addresses data ownership by the Government and/or by the contractor
- FAR Subpart 24.3 et al.-Privacy Training
  - FAR Clause 52.224-3 Privacy Training

☐ 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.

Monitoring will primarily target users with privileged accounts, such as system administrators who can change configuration settings or escalate access permissions or roles; however, login history is recorded for all users, and field history tracking is recorded for select data fields, including some PII data elements.

SEP is not intended for monitoring users, however, the system does identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about a user's visit, including time/date, verification attempt ID, username, identity verification method, action attempted, status of the attempt, IP address, and location, as well as create/update/delete activities performed by users to support user access controls, troubleshooting, and incident response support. Audit logs may also be used to identify unauthorized access or monitoring.

☐ No

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

Login history collects information for detecting and resolving authentication or login issues. This includes information for assisting users in accessing their accounts or for researching unauthorized access attempts. Information collected may include data such as time, verification attempt ID, username, identity verification method, action attempted, status of the attempt, IP address, and location.

Field history tracking will be applied to sensitive data elements or elements that, if subject to unauthorized change, could present a risk to identity authentication or to the mission or business process. For example, these elements may include name, email, phone number, birth date, and dependent information to detect any instance of change by an unauthorized person.

A minimum number of system administrators will be able to access platform configuration settings, and all platform configuration settings will be monitored for changes. All privileged accounts will be monitored and routinely audited.

The Volunteer.gov web site may use session cookies for technical purposes to record encrypted authentication information for the duration of a specific session. The session cookie does not include the user's username or password and does not store other confidential user and session information.

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

Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring. Procedures are published for granting accounts, and privileged accounts are routinely audited for compliance.

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 Deputy AD/Deputy ACIO, Information Resources, National Park Service, serves as the Information System Owner for the Stewardship Engagement Platform and the official responsible for oversight and management of security controls and the protection of customer agency information processed and stored by the SEP system. The Information System Owner and the NPS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in SEP, in consultation with the NPS Associate Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The SEP Information System Owner is responsible for the daily operational oversight and management of the security and privacy controls, for ensuring the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The SEP Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and appropriate NPS and DOI officials in accordance with NPS and DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer.