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: Youth Partner Portal
Bureau/Office: National Park Service, Workforce & Inclusion Directorate

Date: December 23, 2021
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, 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 21st Century Conservation Service Corps (21CSC) is a major National Park Service (NPS) youth and young adult program. This program provides employment opportunities on natural and cultural resources conservation projects in national parks and program offices. Non-profit youth serving organizations (known as service and conservation corps) recruit participants through their organizations to work on these projects. These projects are collaboratively designed and

developed jointly by the participating NPS park and/or office with the organization.

The NPS 21CSC Program spends between $31- $41 million on projects across the country. An additional $5-$10 million is matched through philanthropic funds. These projects are executed in all states and territories. The 21CSC program needs to collect personally identifiable information (PII) which allows the NPS in collaboration with its' partner organizations to conduct recruitment, placement, tracking, and management of the program participants.

NPS Youth Partner Portal is a new application developed to capture the following information for projects hosted at various NPS locations and funded by NPS under a master cooperative/task agreement with a partner organization:

- Partner related public information
- Projects that each partner is currently involved with for NPS
- Participant details for all participants enrolled by the partner
- Participant's involvement in projects and the hours spent by them performing specific types of work.

This information will be used by NPS to generate reports that satisfy the requirements laid out by the John D. Dingell, Jr, Conservation, Management, and Recreation Act of 2019 for congressional reporting of information regarding 21CSC programs.

21CSC partners are local and national non-profit organizations that work in partnership with the NPS to provide services, training, education and employment opportunities for teens and young adults from 16-30 years old and military veterans up to the age of 35 years old. The following link provides the list of 21CSC partner organizations which is maintained on the NPS website: https://www.nps.gov/subjects/youthprograms/21st-century-conservation-service-corps-opportunities.htm.

The partner organization users are authenticated through Login.gov. Login.gov is a GSA provided FedRAMP approved authentication service specifically designed for external organizations and users to access government applications as partners or customers. After users are authenticated via Login.gov, NPS will register these users in the system using their name and email address which will provide them access to the Youth Partner Portal. Once logged in to the Youth Partner Portal, these users will either perform data entry or upload bulk data based on the information that they directly collected from the participants related to the projects they worked on, such as the participants' PII information as well as the number of hours spent on the project.

C. What is the legal authority?

- 21st Century Conservation Service Corps Act (21CSC), March 12, 2019
- John D. Dingell, Jr, Conservation, Management, and Recreation Act of 2019
- 16 U.S.C. §1281(e) The Wild and Scenic Rivers Act

- 16 U.S.C. § 1246(h)(1) Agreements to Operate, Develop, and Maintain Portions of National Trails
- 16 U.S.C. § 1723(c)(1) Public Land Corps
- 16 U.S.C. §l 7j-2(e) authorizes the NPS to expend funds for educational lectures in the vicinity of and with respect to national parks and for the services of employees in cooperation with nonprofit, scientific, and historical societies engaged in educational work in parks.
- 16 U.S.C. §4601 -1, Subsection (f)(l) authorizes the NPS to sponsor, engage in, and assist in research relating to outdoor recreation, directly or by contract or cooperative agreements, and make payments for such purposes. Subsection (f)(2) authorizes NPS to undertake studies and assemble information concerning outdoor recreation, directly or by contract or cooperative agreement, and to disseminate such information. Subsection (f)(3) authorizes cooperation with educational institutions and others to assist in establishing programs and activities to encourage public use and benefits from outdoor recreation (funds may even be advanced if in the public interest).
- 16 U.S.C. §1246(h)(l), National Trails System Act, authorizes cooperative agreements with states or their political subdivisions, landowners, private organizations, or individuals to operate, develop, and maintain portions of national trails located within or outside the boundaries of a federally administered area.
- 54 U.S. Code § 101701(b). Challenge cost-share agreement authority (Pub. L. 113–287, §3, Dec. 19, 2014, 128 Stat. 3134; Pub. L. 113–40, §10(c), Oct. 2, 2013, 127 Stat. 546.)
- 54 U.S. Code § 101702(a) - Cooperative agreements, (a) Transfer of Service Appropriated Funds - A cooperative agreement entered into by the Secretary that involves the transfer of Service appropriated funds to a State, local, or tribal government or other public entity, an educational institution, or a private nonprofit organization to carry out public purposes of a Service program is a cooperative agreement properly entered into under section 6305 of title 31.
- 16 U.S.C. 470 – National Historic Preservation Act (NHPA) Legislation
- Federal Regulations - 2 C.F.R. § 200, 2 C.F.R. § 1402
- 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 code: 010-000002835; Youth Partner Portal 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.*
None			

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

☒ Yes

Volunteer records are covered under DOI-05, Interior Volunteer Services File System (May 23, 2001, 66 FR 28536); modification published 86 FR 50156 (September 7, 2021).

Records on Federal employees are covered under OPM/GOVT-1, General Personnel Records, December 11, 2012, (77 FR 73694); modification published November 30, 2015 (80 FR 74815). Records involving the administrative or operational relationships between the employee and the office in which the employee works are covered under DOI-58, Employee Administrative Records (April 20, 1999, 64 FR 19384); modification published February 13, 2008, 73 FR 8342 and 86 FR 50156 (September 7, 2021).

Records on applicants for Federal employment are covered under OPM/GOVT-5, Recruiting, Examining, and Placement Records (March 26, 2014, 79 FR 16834); modification published November 30, 2015 (80 FR 74815).

DOI Personal Identify Verification (PIV) credentials are covered under DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) (March 12, 2007, 72 FR 11040); modification published 86 FR 50156 (September 7, 2021).

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: *Describe*

OMB Control Number 0596-0247, Public Land Corps Tracking Sheet, Expiration Date: 02/28/2022

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Gender
☒ Birth Date
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Education Information
☒ Military Status/Service
☒ Race/Ethnicity
☒ Other:

The purpose of the PII data being collected is for reporting requirements under the Dingell Act. The information may also be used to determine participant eligibility for hiring based on the total hours spent by the participant under the Research Assistant Program (RAP). In addition to the data elements selected above, the following participant data is collected:

- Participant hours worked and NPS work location
- Career goals, skills and abilities
- Certificate status and date of completion
- Are participant hours attributed towards Conservation Fellow Program Direct Hiring Authority for Resource Assistant (DHA-RA)?
- Narrative/comments specific to participant's work on a particular project
- Permanent address zip code only
- Birth date month and year only

Partner organizations are required to complete and maintain an I-9 Employment Eligibility Verification form which includes parental consent for participants under the age of 18. Partner organizations are required to affirm in the system that they have received parental consent for participants under 18.

Partner point of contact information is collected from the partner organization. The system collects the authorized partner organization user's name and email address for purposes of account management.

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:

Partner organizations will collect information from individual participants and import or input the participants' information to the system. Partner organizations also input Partner point of contact information. Individual participants do not have access to the system to provide information directly.

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*

Access to the Youth Partner Portal requires authentication of partner organization users through Login.gov.

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

PII collected will be used to support reporting required by Congress via the Dingell Act for 21CSC program related projects that were managed by the partner organizations and the summary statistical reporting for the number of hours, total gender distribution, as well as ethnicity and race distribution. The PII will also be used to determine eligibility status based on number of hours spent by a participant.

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

☒ Within the Bureau/Office:
Youth Partner Portal will be used across all NPS parks, programs, and offices to provide a summary report on 21CSC program related projects, hours, gender, ethnicity, and race data. The tracking and data entry will be done externally by partner organizations.

To gain access to the Youth Partner Portal, users will need a profile in Login.gov and an assigned security role within the Youth Partner Portal application. Users will be allowed access to information based on their role.

☒ Other Bureaus/Offices:

Youth Partner Portal may be used across DOI bureaus and offices to provide a summary report on 21CSC program related projects, hours, gender, ethnicity, and race data.

☐ Other Federal Agencies

☐ Tribal, State or Local Agencies

☒ Contractor:
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 hosts 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.

☒ Other Third-Party Sources:
Partner organizations who will be performing the 21CSC projects under a master agreement with NPS will have access to the PII. The partner organization users will be granted access to the Youth Partner Portal via their Login.gov profile and a role assigned within the Youth Partner Portal. Partner organizations will provide the PII data via data entry or bulk upload within the Youth Partner Portal and will only have access to the data and PII for their programs based on their access permissions.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes

Individuals voluntarily provide information to the Partner Organization when applying for a 21CSC project, internship, or the RAP through the partner's platforms. The partner organizations are responsible for recruiting and collecting PII information from the individuals that will be working on park/office projects hosted at various NPS locations and are funded by NPS under a master cooperative/task agreement with the partner organization. An individual can decline to share their information with the partner organization by not completing the application, however, they will not be able to take advantage of the on-the-job developmental opportunity with NPS through the 21CSC programs. Furthermore, for data related to gender and ethnicity, the individual may choose not to provide a response.

☐ No

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

☒ Privacy Act Statement:

A link to a Privacy Act Statement will be provided when collecting PII, such as point of contact information, from the Partner Organization users. NPS will request that Partner organizations provide a Privacy Act Statement to participants when collecting their information, as appropriate.

☒ Privacy Notice:

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

☒ Other:

Users will be 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, user ID, and record ID. Summary reports can be retrieved by Fiscal Year, Date Range, Location and/or Partner Organization Name.

I. Will reports be produced on individuals?

☒ Yes

Reports are only generated on aggregated statistical information for the purpose of reporting youth engagement activities to Congress. Eligibility reports will be generated to determine eligibility of individuals for hiring based on number of hours completed. This report will only contain an individual's system generated unique identifier, first name, last name and their eligibility status. These reports will only be accessible to specific users based on roles assigned.

☐ No

Section 3. Attributes of System Data

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

The PII information will be entered or bulk uploaded by the Partner Organization users to the Youth Partner Portal. The Partner Organizations are collecting the PII information directly from individuals, so it is assumed to be accurate. To the extent practicable, data entry validations will be implemented to ensure data integrity. Federal agency staff, during the application and user management processes can verify that the information provided is accurate and complete and may request the individual update or correct pertinent data. While performing data entry using the website, data validations will ensure that the correct type of information is being entered. For bulk uploads, a validation process will ensure that all data is in valid format and size, as well as the data relations will be verified before loading the data.

B. How will data be checked for completeness?

Partner Organizations, while collecting PII information directly from individuals, will ensure all necessary information are obtained and is complete. To the extent practicable, data entry validations will be implemented to ensure data integrity. Federal agency staff, during the application and user management processes will verify information provided for accuracy and completeness. When importing bulk data, the import will only progress if all related data is provided at the same time. When data entry is performed using the website, users will not be able to save the information until all required fields have been completed.

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

Partner Organization users will be required to update and provide new information at a set interval of time within the Youth Partner Portal. This set time period will be called the reporting deadline for the partners and is outlined in their task agreement. The system stores and displays the last modified date as well as last modified user information.

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

Youth Partner Portal 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 (NARA) (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 destroyed/deleted 7 years after closure. The disposition for routine interpretation and education records is temporary and records are destroyed/deleted 3 years after closure.

Records and data collected, created, or generated by other organizations or by individuals working for the NPS under contracts, interagency agreements, cooperative agreements, or other agreement instruments with the NPS, including research permits, are considered NPS records unless the contract, agreement, or permit specifically provides otherwise. All agreements, contracts, or permits will clearly state this. Copies or originals of all project documents and data generated pursuant to these agreements will be obtained and retained by the NPS office managing the project. Failure of organizations or individuals to provide the Service with data obtained while working in NPS units within the agreed-upon time period may adversely affect such organizations or individuals' access to Federal lands in the future.

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 Departmental policy.

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 privacy risks to individuals are considered moderate due to the types of PII collected. Multiple controls have been implemented to mitigate and substantially lower privacy risks. Data entry is only performed through the Youth Partner Portal web application by the partner organizations using data entry website or bulk import feature. Youth Partner Portal will be protected by encryption to safeguard the data both while in transit and at rest. Web applications follow defined application security roles and permissions to ensure proper distribution and disclosure of information guided by the principle of least privilege to minimize the risk of improper information disclosure. Disposition of all information are guided by the NPS Records retention schedules.

A formal Assessment and Authorization for issuance of an authority to operate will be conducted in accordance with the Federal Information Security Modernization Act (FISMA), and the system will be 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.

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 are referenced in the System Security and Privacy Plan. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

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, the system incorporates the use of role-based permission to give access to limited sets of PII. Access to data is restricted to authorized personnel who require access to perform their official duties. Youth Partner Portal enables access for all users using Login.gov multifactor authentication mechanism. Transport Layer Security (TLS) technology is employed to protect information in transit using server authentication. Database level encryption has been deployed to encrypt database files at rest. Device level encryption has been deployed to encrypt data at rest on laptop computers. 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 of data interception in transit between the user's web browser and the application server. This risk is mitigated by encryption of data in transit.

There is a risk that user 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 security, privacy, and records management as well as role-based training where applicable and sign the NPS 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 a risk that information in the system will be maintained longer than necessary to achieve the agency's mission or may be improperly disposed or destroyed. 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. Detailed procedures and automated scripts for data disposal/destruction will be developed and secured under change management. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

There is a risk that information including PII may be output from users' web browser and improperly secured or disposed. All PII information including reports is access-controlled, and only NPS staff with the appropriate need-to-know will be given access. DOI mandates that all Federal employees and contractors complete initial and annual information security and privacy training. The resulting high awareness provides an enhanced level of assurance on the life cycle management of the PII data. Physical media including printed reports is manually collected and secured following the program-defined process for ensuring chain of custody and appropriate safeguards until the physical media is disposed of by shredding or pulping for paper media or erasing or degaussing for electronic physical media.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA, applicable SORNs, and Privacy Act Statements within the application. NPS will request that Partner organizations provide a Privacy Act Statement to participants when collecting their information, as appropriate.

There is a risk of lack of consent from participants under the age of 18. Partner organizations are required to complete and maintain an I-9 Employment Eligibility Verification form which includes parental consent for participants under the age of 18. Partner organizations are required to affirm in the system that they have received parental consent for participants under 18.

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

The agency is authorized to collect the project and demographic information from the partner organizations via an OMB approved form, OMB Control Number 0596-0247. This information is both relevant and necessary as it is used to provide reporting to congress and satisfy the requirements of the Dingell Act. This reporting includes summary accomplishments and demographic information on work performed by the participants via the partner organizations. The data will also help track various eligibility criteria for the Direct Hire Authority and Public Lands Corp hiring authorities.

☐ 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?

New data is not created or derived by the system.

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: *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.

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 users who have permissions to add/update the information and not by other users or by other partner organizations. 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

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 are 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.

NPS contractor staff are 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 published procedures.

☐ 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

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.

Youth Partner Portal 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.

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.

☒ 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.

☒ 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.

☒ 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.

Chief, Youth Programs Division serves as the Youth Partner Portal Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in the Youth Partner Portal. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within the system, in consultation with NPS and DOI Privacy Officials.

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 Youth Partner Portal Information System Owner and Youth Partner Portal Information System Security Officer are responsible for daily operational oversight and management of the security and privacy controls, for ensuring to 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 Youth Partner Portal 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 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.