Appendix A: DI-4001 PIA Form

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: NPS Common Learning Portal

Date: October 15, 2015

Bureau/Office: National Park Service

Bureau/Office Contact Title: Program Manager

Point of Contact
Email: Dale_Carpenter@nps.gov
First Name: Dale
M.I.:
Last Name: Carpenter
Phone: 304-535-6401
Address Line 1: 252 McDowell Street
Address Line 2:
City: Harpers Ferry
State/Territory: WV
Zip: 25425

Section 1. General System Information

A. **Is a full PIA required?**
This is a threshold question. Indicate whether the system collects, maintains, uses or disseminates information about members of the general public, Federal employees, contractors, or volunteers. If the system does not contain any information that is identifiable to individual (e.g., statistical, geographic, financial), complete all questions in this section and obtain approval and required signatures in Section 5. The entire PIA must be completed for systems that contain information identifiable to individuals, including employees, contractors and volunteers.

☒ 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?
Describe the purpose of the system and how it relates to the program office's and Department's mission. Include the context and background necessary to understand the purpose, the name of the program office and the technology, project or collection being assessed.

The NPS Common Learning Portal (CLP) will serve as a common location for advertising national, regional, and park specific training events to NPS employees. The CLP is focused on increasing the visibility of training available to NPS employees and is also making the site available to the public to allow NPS partners, retired NPS employees, and other interested persons not directly affiliated with the NPS access. The CLP also establishes communities of practice using interest groups and forums in order to increase communication among the NPS training community.

The CLP includes an "Ask the Expert" feature where industry experts or retired NPS employees who are experts in their field can field questions from NPS employees. Individuals may visit the Common Learning Portal to learn about upcoming training events without providing any information. However, in order to participate in community forum discussions, an account on the site must be created. Registering for an account requires the user provide the following information for use in the community discussion forums:

- Name
- Email address, and
- Username.

Once registered, the user has the opportunity to voluntarily provide additional information on their portal profile, to include:

- Photo (optional)
- Title
- Location,
- Expertise,
- Duties, and
- Additional personal information such as hobbies or activities.

Additional information provided by the individual in these text fields such hobbies or activities in general are unbeknownst to us; however we reserve the right to remove offending information from the portal at any time.

C. What is the legal authority?

A Federal law, Executive Order of the President (EO), or DOI requirement must authorize the collection and maintenance of a system of records. For Privacy Act systems, the response should reflect the information provided in the authority section of the Privacy Act system of records notice.

54 U.S. Code § 101321 - Service employee training; and 54 U.S. Code § 101322 - Management development and training

D. Why is this PIA being completed or modified?

Indicate why the PIA is being conducted. For example, the system is being significantly modified or two systems are being merged together.

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

010-000001975 - Common Learning Portal

□ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Enter "None" if no subsystems or applications are hosted. For General Support Systems (GSS) be sure to include all hosted major applications, minor applications, or other subsystems, and describe the purposes and types of PII if any. Privacy risks must be identified and adequately addressed for each hosted application or subsystem identified in the GSS PIA. A separate PIA should be conducted for each hosted application or subsystem that contains PII to ensure privacy implications are assessed. In any case, the GSS PIA must identify all hosted applications, describe the relationship, and reference or append the PIAs conducted for the hosted applications. The GSS PIA and associated PIAs must be reviewed and approved by all *officials as appropriate; and all related PIAs, SORNs and supporting artifacts must be entered into CSAM.*

There are no minor systems or subsystems that are hosted on this system.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
N/A	**N/A**	N/A	**N/A**

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

A Privacy Act SORN is required if the information system or electronic collection contains information about individuals that is retrieved by name or other unique identifier. Provide the DOI or Government-wide Privacy Act SORN identifier and ensure it is entered in CSAM for this system. For new SORNS being developed, select "Yes" and provide a detailed explanation. Contact your Bureau Privacy Officer for assistance identifying the appropriate Privacy Act SORN(s).

☒ Yes: *List Privacy Act SORN Identifier(s)*

Common Leaning Portal - NPS 31

□ No

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

The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact your Bureau Information Collection Clearance Officer for assistance to determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.

☒ Yes: *Describe* A proposed information collection notice was submitted to OMB on 01/15/2016.

□ No

Section 2. Summary of System Data

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

Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.

☒ Name
□ Citizenship
□ Gender
□ Birth Date
□ Group Affiliation
□ Marital Status
□ Biometrics
□ Other Names Used
□ Truncated SSN
□ Legal Status
□ Place of Birth
□ Religious Preference
□ Security Clearance
□ Spouse Information
□ Financial Information
□ Medical Information
□ Disability Information
☒ Other: *Specify the PII collected.* handle (forum username)

□ Credit Card Number
□ Law Enforcement
□ Education Information
□ Emergency Contact
□ Driver's License
□ Race/Ethnicity
□ Social Security Number (SSN)
□ Personal Cell Telephone Number
□ Tribal or Other ID Number
☒ Personal Email Address
□ Mother's Maiden Name
□ Home Telephone Number
□ Child or Dependent Information
□ Employment Information
□ Military Status/Service
□ Mailing/Home Address

Individuals may visit the Common Learning Portal to learn about upcoming training events without providing any information. However, in order to participate in community forum discussions, an account on the site must be created; registering for an account requires the user provide their name, email address, and create a handle or username for use in the community discussion forums.

Once registered, an internal user identifier is assigned automatically by the system. The user has the opportunity to voluntarily provide additional information on their portal profile. The portal profile consists of a photo and five information fields: title, location, expertise, duties, and an "about" text field. Additional information provided by the individual in this text field is unbeknownst to us; however we reserve the right to remove offending information from the portal at any time.

B. What is the source for the PII collected? Indicate all that apply.
Include all sources of PII collected. For example, information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, from a computer readable extract from another system, or may be created within the system itself. If information is being collected through an interface with other systems, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.

☒ Individual
□ Federal agency
□ Tribal agency

☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.
Indicate all the formats or methods for collecting PII that will be used. If the system receives information from another system, such as a transfer of financial information or response to a background check, describe the system from which the information originates, how the information is used, and how the systems interface.

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems
☐ Other: *Describe*

D. What is the intended use of the PII collected?
Describe the intended uses of the PII collected and maintained in the system and provide a detailed explanation on how the data will be used. The intended uses must be relevant to the purpose of the system; for Privacy Act systems, uses must be consistent with the published system of records notice.

PII collection is for the purpose of registering an account on the portal; portal registration requires a name, email address, and handle (forum username). Once registered, users may share additional information on their portal profile page; registration on the portal and submitting portal profile information is completely voluntary. Registration is required for participating in community forums. Other than providing a means for registration, NPS Learning and Development have no other use for the PII collected.

Although NPS does not collect, maintain or disseminate PII from users of the portal, there may be instances where PII becomes available. For instance, if there is evidence of criminal activity or a threat to the government, such information may be turned over to the appropriate authorities for further action.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.
Indicate all the parties, both internal and external to DOI, with whom PII will be shared. Identify other DOI offices with assigned roles and responsibilities within the system, or with whom information is shared, and describe how and why information is shared. Also, identify other federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared; and describe any routine information

sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. If sharing is pursuant to a Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for the disclosure is maintained.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

NPS Learning and Development will manage the portal and use site metrics to improve content and portal navigation; metrics may include the number of registered users.

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

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

☐ 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.*

☐ 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?
If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individual opportunity to consent to or decline the collection or provision of personal information occurs at the time of registration. Providing the information to NPS is voluntary, however, failure to provide the requested information may impede individual's registration.

☐ 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.

Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

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

A Privacy Act Statement will be provided on the registration page of the portal.

☒ Privacy Notice: *Describe each applicable format.*

A privacy notice will be provided on the front page of the portal.

☐ Other: *Describe each applicable format.*

☐ None

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

Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Are specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).

Email address or an internal user identifier assigned automatically by the system could be used to retrieve information on a user as both information types are considered unique. Data retrieval will be performed by the portal systematically in order to authenticate users and display information related to them, such as their profile page or portal pages that they have favorited.

I. Will reports be produced on individuals?

Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many systems have features that allow reports to be generated on data in the system or on user actions within the system.

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

☒ No

Section 3. Attributes of System Data

A. **How will data collected from sources other than DOI records be verified for accuracy?**
Data accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. The information has to have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.

Among the data collected from users, only their email address needs to be verified for accuracy. This verification will occur while creating an account; a system generated email will be sent to the user who will then need to click on a link in the email to verify their email address. Other information provided by the user will not require verification. NPS relies on the accuracy of the information provided to it by the individual user.

B. **How will data be checked for completeness?**
Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.

The user’s email address requires verification as the email address is used to send notices to the user and assists in the portal authentication process. Verification will occur after registering an account; an email will be sent to the email address provided by the user who will then need to click on a link in the email to verify access to the provided email address. Other information provided by the user does not require verification.

C. **What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).**
Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and analysis. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

The system or administrators will not attempt to ensure user provided data is current, it is the responsibility of the user to maintain the accuracy of their information; NPS relies on the information provided to it by the individual user to ensure the data is current.

D. **What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.**
Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Information system owners must consult with Bureau/Office Records Officers early in the development process to ensure that appropriate retention and destruction schedules are identified, or to develop a records retention schedule for the records contained in the information system. Be sure to include applicable records retention

schedules for different types of information or subsets of information and describe if subsets of information are deleted and how they are deleted.

Records in this system are maintained in accordance with the National Park Service Management and Accountability (Item 10), D. Housekeeping and Supporting Records Record Schedule (N1-79-08-9) which has been approved by the National Archives and Records Administration. Records are temporary and 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?

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, the Departmental Manual, bureau/office records management policies, or standard operating procedures.

Records in this system are maintained in accordance with the National Park Service Management and Accountability (Item 10), D. Housekeeping and Supporting Records Record Schedule (N1-79-08-9) which has been approved by the National Archives and Records Administration. Records are temporary and destroyed/deleted 3 years after closure.

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.

Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy risks. Provide an example of how information is handled at each stage of the information life cycle. Also discuss privacy risks associated with the sharing of information outside of the Department and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department.

The risk is mitigated by the security and privacy controls implemented to safeguard privacy and the limited collection of personally identifiable information from individuals. The system is hosted in a certified Federal Risk and Authorization Management Program (FedRAMP) cloud-based environment employing security and privacy controls defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The system cloud-based environment meets FedRAMP and Federal Information Security Modernization Act (FISMA) Moderate compliance standards.

Collection of information is for the sole purpose of authenticating users to the site; for this we require their name and email address. Site visitors who choose not to register will still be permitted to view upcoming training events and information; registration is a system requirement necessary to participate in the group discussion forums.

Access to data collected, stored and utilized is limited to system developers and administrators, and authorized program officials. Data shared outside of the system will be limited to derived summary reports that do not contain personally identifiable information.

Records are destroyed in accordance with approved methods as outlined in DOI policy and the applicable records schedule.

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?

Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system? For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order of the President.

☒ Yes: *Explanation* The use of user provided data enables a richer more engaging experience for the user in the form of community discussion forums and interacting with other users pursuing professional development or the development of training materials.

□ No

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

Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data. Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

□ 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?

Will the results or new data be placed in individuals' records? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?
Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?
Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy. Also explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

Only the user's email address is verified for relevance and accuracy. It requires verification as the email address is used to send notices to the user and assists in the portal authentication process. Verification will occur after registering an account; an email will be sent to the email address provided by the user who will then need to click on a link in the email to verify access to the provided email address. Other information provided by the user does not require verification for relevance and accuracy.

F. Are the data or the processes being consolidated?
If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of identification and authentication that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

☐ 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. *Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to make changes in the system? Also consider "other" users who may not be as obvious, such as the GAO or the Inspector General, database administrators, website administrators or system administrators. Also include those listed in the Privacy Act system of records notice under the "Routine Uses" section when a Privacy Act system of records notice is required.*

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*

Visitors may view the portal (system) anonymously and browse information on upcoming training events and discover training resources. However, registering an account is necessary in order to participate in the community discussion forums.

<u>Unregistered portal users:</u> Individuals who browse the portals information without registering for an account; access is strictly read-only with no access to the community discussion forums.

<u>Registered portal users:</u> Individuals who have registered for a portal account have read-only access to the site, except where they are permitted to contribute to community discussion forums, comments on topics or posts, or editing their own information such as the portal profile page.

Registered users who are responsible for content development and publishing can be assigned additional permissions through the use of roles. Roles outline levels of permission and access to administrative areas of the portal. Portal roles will include author, content approver, master content approver, and administrator. Portal administrative areas allow content to be developed, published and archived; as well as manage users and site functions.

<u>Underlying support system users:</u> Individuals who are responsible for maintaining the infrastructure that the portal resides within and have administrator access. Infrastructure encompasses the cloud hosting platform where the servers reside, the server system accounts which include the operating system and relational database services. Administrator access to infrastructure services is controlled by the cloud provider who is contractually obligated to

maintain the security of the infrastructure through the use of technology, role separation, and staffing.

Visitors access the site via a web browser, this access is encrypted by a Secure Sockets Layer (SSL) connection. Site administrators also have access to the site via encrypted Virtual Private Network (VPN) connection to administer the servers. This VPN connection is also used to authenticate NPS employees via the DOI’s Active Directory service; employees in Active Directory will authenticate (login) to the site using their Active Directory credentials.

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

Users are normally only given access to certain data on a “need-to-know” basis for information that is needed to perform an official function. Care should be given to avoid “open systems” where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when users may not need to have access to all the data. For more guidance on this, refer to the Federal Information Processing Standards [FIPS] Publications in the authorities section. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of applying logical access controls, which are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of information system owners to ensure no unauthorized access is occurring.

The purpose of the portal is to advertise training events and promote collaboration among training development professionals, as such much of the data within the system can be accessed freely via the Internet; access is restricted to the community discussion forums which require registering for an account. Users who register with a @nps.gov email address are provided with access to content which has been tagged as “NPS Only” by the content or program manager.

Access to the portal data at the infrastructure level is restricted to authorized system administration functions such as database and web server backups.

Access to records in the system is limited to authorized personnel whose official duties require such access; authorized personnel are required to complete annual Federal Information Systems Security Awareness and Privacy and Records Management (FISSA) training and sign the DOI Rules of Behavior. Electronic data will be protected through user identification, encrypted passwords, database permissions and software controls. All data, including PII, delivered to and from an individual’s web browser will be encrypted using approved federal encryption protocols. These security measures will establish different degrees of access for different types of users.

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 involved in the design and development of the portal and privacy clauses were not included in their contract.

Contractors are responsible for hosting the portal and the following clauses were included in the DOI cloud hosting contract:

FAR 52.204-9 Personal Identity Verification of Personnel (JAN 2011)
FAR 52.224-1 Privacy Act Notification (APR 1984)
FAR 52.239-1 Privacy or Security Safeguards (AUG 1996)

The Cloud Services Provider (CSP) has employed the security and privacy controls defined by NIST SP 800-53, and meets FedRAMP and FISMA Moderate compliance standards and are audited regularly in SOC 2, Type II reports.

□ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?
Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

□ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?
Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

☒ Yes.

The system can *identify* registered portal users by their unique user identifier assigned during registration; this identifier is a number that is not normally visible or known to the user.

The system can *locate* the activity of registered portal users who add content to the portal which may be in the form of comments, posts, updating profile information, forum discussions, ratings, and reviews. When a registered user performs a function such as these, a record of that activity is created, in the form of web content, and is attributed to them.

The system does not actively *monitor* portal users and is not programmed to do so.

□ No

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

The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) detail how audit logs should be used for DOI systems. Provide what audit activities are maintained to record system and user activity including invalid logon attempts and access to data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication of users to the system. Examples of information collected may include username, logon date, number of failed logon attempts, files accessed, and other user actions on the system.

The system does not actively monitor portal users and is not programmed to do so. Audit logs are maintained in the system and track login attempts and errors.

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

Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.

The portal's governance plan outlines the roles and responsibilities of portal users with elevated access to the portal administration functions. The outline uses the principle of least privilege in order to provide only the level of access required to perform in their role. Privacy Act notices and continuous system monitoring notices will be posted prominently.

The portal's infrastructure contract provides continuous monitoring, vulnerability management, contingency planning, FISMA compliance, intrusion detection, incident response, forensic analysis, and assessment and authorization (A&A).

N. How will the PII be secured?

Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do the audit features include the ability to identify specific records each user can access? How is the system audited? For example, does the system perform self audits, or is the system subject to third party audits or reviews by the Office of Inspector General or Government Accountability Office (GAO). Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy and security training is provided to system users. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.

(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*

The Cloud Service Provider's (CSP) Federal Data Centers (FDCs) employ various levels of security controls including perimeter protection, armed security guards, personnel ID badges, and separate access controls at each facility. The CSP provides access to facilities and information systems strictly on a “need to know” basis and practices the principle of least privilege. In addition, daily operations consisting of opening and closing, closed areas, safes, and arming and disarming the intrusion detection system must have completed paperwork associated with each task at the end of each day.

(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*

All user accounts within the portal and supporting infrastructure require strong passwords and user identification. The CSP firewall provides secure access to the portal as well as point-to-point VPN connectivity from the client Trusted Internet Connection (TIC). Access to the web-based administration tools can be restricted to source connections originating from the TIC. The CSP is also responsible for monitoring for intrusion detection. All connections to the portal will be encrypted using SSL/HTTPS technology which also enables the Public Key Infrastructure; VPN connections to the infrastructure are also encrypted.

(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 CSP uses FedRAMP certified geographically isolated Federal data centers to host and secure backups at multiple locations. It employs the security and privacy controls defined by NIST SP 800-53, and all data centers for Government use meet FedRAMP and FISMA Moderate compliance standards and are audited regularly in our SOC 2, Type II reports; they also use the application Syslog for infrastructure logging and audit compliance. Role based training is outlined in the portal governance document where roles and processes are defined. DOI employees are required to pass mandatory Security, Privacy and Records Management Training annually.

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.

Although all employees who have access to information in a Privacy Act system have responsibility for protecting and safeguarding that information, often the information system owner and Privacy Act system manager share the responsibility for protecting the privacy rights of employees and the public. For Privacy Act responsibilities refer to 383 Department Manual Chapters 1-13 and DOI Privacy Act regulations at 43 CFR Part 2. Also, describe how Privacy Act complaints and requests for redress or amendment of records are addressed.

The information system owner and NPS Privacy officer share the responsibility of protecting the privacy rights of the public and employees. Privacy Act complaints and requests for redress will be handled jointly between these two entities.

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?

This may be the information system owner and Privacy Act system manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in language contained in an agreement (e.g., Head of the Bureau or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.

There are potentially several parties responsible for assuring the proper use of data and reporting potential Privacy Act violations or unauthorized access; the core responsible parties include the system owner, NPS Privacy officer, and NPS Information Technology Security office (ITSO).

Section 5. Review and Approval

Appendix A – DI-4001 PIA Form

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the DOI Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

Information System Owner

Email: Dale_Carpenter@nps.gov
First Name: Dale M.I.: Last Name: Carpenter Title: Distance Learning Group Manager
Bureau/Agency: National Park Service Phone: 304-535-6401 Date:

Signature:

Information System Security Officer

Email: ryan_jennings@nps.gov
First Name: Ryan M.I.: Last Name: Jennings Title: Web Products Manager
Bureau/Agency: National Park Service, Learning and Development Phone: 304-535-5057Date:

Signature:

Privacy Officer

Email: teri_barnett@ios.doi.gov
First Name: Teri M.I.: Last Name: Barnett Title: Departmental Privacy Officer
Bureau/Agency: Office of the Chief Information Officer Phone: 2022081943 Date:

Signature:

Reviewing Official

Email: Shane_Compton@nps.gov
First Name: Shane M.I.: Last Name: Compton Title: Associate Director, Information Resources
Bureau/Agency: National Park Service Phone: 2022082433 Date:

Signature: