**U.S. Department of the Interior**
PRIVACY IMPACT ASSESSMENT

## Introduction

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

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

**Name of Project:** NPS Common Learning Portal
**Bureau/Office:** National Park Service
**Date:** 4/11/19
**Point of Contact:**
Name: Felix Uribe
Title: Associate Privacy Officer
Email: felix_uribe@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 National Park Service (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?

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?

☒ 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.**

| **Subsystem Name** | **Purpose** | **Contains PII** *(Yes/No)* | **Describe** *If Yes, provide a description.* |
|---|---|---|---|
| **NONE** | **N/A** | N/A | **N/A** |

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

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

DOI-16, Learning Management System, 83 FR 50682 (October 9, 2018)

□ No

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

☒ Yes: *Describe*

The Information Collection Request for the Common Learning Portal was approved by OMB in March 2017. The control number is 1024-0284. It does not expire until 03/31/2020.

□ No

## Section 2. Summary of System Data

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

☒ Name
☒ Personal Email Address
☒ Other: handle (forum username)

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.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

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

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

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

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.**

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

PII will not be shared with outside organizations and will not be included in internal reports. Reports will be generated and shared with the NPS Workforce & Inclusion Directorate leadership, which includes the Learning & Development division, of which the hosting program, NPS Distance Learning Group, is a member. These reports will include general site usage metrics and not be focused on individuals or include PII. The reports will provide information on how the site is being used by employees, adoption rate, geographic location of connections, page views, and additional site analytics provided by Google Analytics.

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

The system may be shared with the Department’s learning management system for employee training management purposes.

☐ 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.*
Contractors have access to the system data as appropriate with their role; the system is hosted by a cloud service provider under the DOI Foundation Cloud BPA and has contractors developing, hosting, and administering the system.

□ 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.*

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.**

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

A Privacy Act Statement will be provided on the registration page and will be available to all users who access the system.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this PIA and the published systems of records notice DOI-16, DOI LEARN (Department-wide Learning Management System), which may be viewed at https://www.doi.gov/privacy/sorn.

□ 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.).**

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?**

☐ 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?**

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?**

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).**

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.**

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.

At the system level, items deleted within the application are sent to the Trash, after 30 days, these items are deleted by the system and removed from the Trash.

At the data level, backups of server data are maintained for 30 days at which time they will be archived for 3 years.

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

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.**

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?**

☒ 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?**

☐ 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?**

N/A. The system does not derive new data or create previously unavailable data about an individual through data aggregation.

**F. Are the data or the processes being consolidated?**

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

**G. Who will have access to data in the system or electronic collection? Indicate all that apply.**

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

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.

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

Registered portal users: 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.

Underlying support system users: 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 Transport Layer Security (TLS) 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?

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?*

Privacy clauses were not included in the original design contract. The current contract (D01 P17PA00060_EK) does include the following Contract Clauses:

SECTION D -- CONTRACT CLAUSES
52.224-1 -- Privacy Act Notification (Apr 1984)
52.224-2 -- Privacy Act (Apr 1984)
52.227-14 -- Rights in Data – General (May 2014)
52.227-17 -- Rights in Data -- Special Works (Dec 2007)

52.245-1 -- Government Property (Jan 2017) Alternate I (Apr 2012).

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)?**

☐ Yes. *Explanation*

☒ No

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

☒ Yes. *Explanation*

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 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?**

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?

(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*

The Cloud Service Provider 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.**

The Program Manager, Distance Learning Group, Office of Learning and Development, Workforce Inclusion Directorate and the NPS Associate 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?**

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 Associate Privacy officer, and NPS Information Technology Security office (ITSO).