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 Library Resource Information Service (LIBRIS)
Bureau/Office: National Park Service
Date: November 4, 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, Reston VA 20192

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ 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 mission of the National Park Service (NPS) Library Information Management (LIM) program is to facilitate efficient management and discovery of library resources held across the NPS by providing NPS libraries (400+) with library profession best practices guidance and current and emerging library standards-based automated technologies, including training and user support.

The purpose of the Library Resource Information System (LIBRIS) is to provide NPS a Cloud-based integrated library system (ILS) to support highly efficient library collections management and search/discovery processes to benefit NPS library personnel and researchers (NPS and external) of varying skill levels. The system is deployed via a Software as a Service (SaaS) suite which is designed specifically for 'special libraries,' i.e., government, nonprofit, legal, and medical. It enables NPS library personnel to perform collaborative cataloging using a central suite of integrated modules and a common Cloud-based database and provides end-users (NPS and external researchers) with fast and sophisticated public catalog search and discovery features for determining and locating relevant resources.

NPS LIBRIS benefits personnel responsible for maintaining NPS libraries and the primary users of resources maintained in NPS library collections, i.e., NPS staff. NPS libraries maintain many formats of materials relevant for multiple NPS job functions, e.g., planning, resource management, and interpretation. As such, the NPS LIBRIS application contributes to achieving the goals and objectives associated with both the DOI mission and the NPS mission.

The public-facing, read-only NPS LIBRIS Online Public Access Catalogue (OPAC) Discovery portal benefits the following individuals:

- Other federal librarians, particularly DOI librarians, as some NPS reports are multi-agency or are otherwise relevant to one or more DOI bureaus and offices. In cases where these agencies need a copy, the NPS LIM team can arrange for a scan of the report to be made, if a digital version is not already available via NPS Denver Service Center's Electronic Technical Information Center (DSC eTIC), or NPS Natural Resource Stewardship & Science's Integrated Resource Management Applications (NRSS IRMA).
- External researchers who can arrange to use library resources on site when able to demonstrate a legitimate research need, and/or if the needed material is an NPS report/study that's non-sensitive and unavailable elsewhere, a scan can be provided upon researcher's request.
- Members of the general public (including students, educators and a wide range of professionals) in that it represents and reveals the wide range of topics associated with the natural, cultural and recreational resources the NPS manages and interprets. In this way, it can serve to stimulate a stewardship ethic and inspire public participation. OPAC End-users may download search results (citations) to submit with a request to their local libraries for borrowing from non-NPS libraries through the Interlibrary Loan (ILL) network service.

C. What is the legal authority?

Secretary's Order 1173, April 1937, and Secretary's Order 2525, Central Library of the Department of the Interior, June 24, 1949; 5 U.S.C. 301, 3101, 5105–5115, 5501– 5516, 5701–5709; 31 U.S.C. 66a, 240– 243; 40 U.S.C. 483(b); 43 U.S.C. 1467; 44 U.S.C 3101; and Executive Order 11807.

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

UII: 010-000000589; **SSP Name:** NPS Library Resource Information Service (LIBRIS)

☐ 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-58, Employee Administrative Records 64 FR 19384 (April 20, 1999); modification published at 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021).

☐ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: Specify the PII collected.

- PATRON RECORDS - Limited to individuals with NPS email addresses who request borrowing privileges. PII collected includes: first name, last name, NPS email address and org code for the individual's NPS affiliated area or office. PII is provided voluntarily by individuals requesting borrowing privileges and is maintained in Patron Records within the Circulation module, which only system administrators and servicing librarians can access. Members of the public, including NPS volunteers, are not accorded borrowing privileges, and therefore Patron Records are not maintained for them.

- USER ACCOUNTS – For authorized library personnel with NPS email addresses, PII collected includes: first name, first letter of last name, NPS email address and org code for the individual's NPS affiliated area or office. For authorized library volunteers without NPS email addresses, PII collected includes: first name, first letter of last name and NPS org code of affiliated NPS unit. This information is used to generate an alphanumeric code for the user as a User Login. PII is provided voluntarily to the User Accounts Manager by individuals wanting a User Account for the NPS LIBRIS Staff portal for performing library collections management and processes. These users require User Login and password to access the staff portal. PII is maintained in the User Accounts area within the Maintenance module (aka 'Admin' module), which only system administrators can access. User Name is an additional field provided in the system to provide a more descriptive identifier of the User Account, since the User Login field is an alphanumeric code.

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 *Describe*
☒ Other: *Describe*

- Individuals requesting borrowing privileges provide needed PII in person or via email.
- Individuals requesting Staff portal access provide needed PII via email.

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

- PATRON RECORDS (Circulation module)
  PII collected is used to track circulation of library materials and hold borrowers accountable for return, repair (if damaged) or replacement (if damaged beyond repair, or lost). PII is maintained via Patron Records managed within the Circulation module, which only the servicing librarians and system administrators can access. Members of the public, including NPS volunteers, are not accorded borrowing privileges, and therefore Patron Records are not maintained for them.

- USER ACCOUNTS (Maintenance module)
  PII collected is used to securely authenticate individuals to the system's Staff portal, manage Staff Account User roles and permissions, and enable auditing of Staff User activities. The information is maintained in User Accounts in the Maintenance module, which can only be accessed by system administrators.

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.*

- PATRON RECORDS (Circulation module)
  Only the three system administrators (comprising the NPS LIM team) and the servicing librarians within NPS have access to Patron Records. The servicing librarians access the Patron Records for routine purposes: creating, updating, or flagging Patron Records for deletion. The System Manager has a periodic need to access the Patron Records area,

involving monitoring of the Patron Records content to ensure appropriate implementation of NPS LIM policies and protocols by the servicing librarians in compliance with required security controls. The information in Patron Records is not shared with anyone.

- USER ACCOUNTS (Maintenance module)
  Only the three system administrators (comprising the NPS LIM team) have access to the User Accounts area. The system administrator assigned the User Accounts Manager role is the only one with a need to access this area on a daily basis for routine User Account Management purposes, e.g., setting up new accounts; deleting accounts; resetting passwords. The System Manager accesses User Accounts on a periodic basis related to the System Manager's role involving monitoring for appropriate implementation of User Accounts Management policies and protocols by the User Accounts Manager in compliance with required security controls. This information is not otherwise shared/used.

☐ 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.*

- Contractor in this context is the proprietor/sole source/Cloud Service Provider (CSP) of the EOS.Web Software-as-a-Service (SaaS), i.e., the vendor-hosted application underlying the NPS LIBRIS application. The Contractor provides licensing, hosting, maintenance, monitoring, system support and 24-7 Client support services.

- Contractor personnel are required to undergo background checks in order to obtain FedRAMP authorization and as defined by NPS policy and procedures. Contractor staff access to PII will be restricted to data on a need to know basis and according to Contractor staff role/function and associated privileges (i.e., only System Support or Client Support staff would be requested by the NPS LIBRIS System Manager or NPS LIBRIS User Accounts Manager to access PII in the event that troubleshooting assistance is required).

- Contractor personnel with privileged accounts are audited, and authentication and other security and privacy controls (including screening, annual privacy and security training, incident reporting, etc.) are enforced as defined in Contractor's System Security Plan (SSP) and Privacy Plan (PP). These measures are critical to protecting the system and the PII contained within it. NPS LIBRIS undergoes a security assessment by a third party assessment organization (3PAO) annually.

☐ 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.*

- PATRON RECORDS (Circulation module)
  Limited to individuals having NPS email addresses who wish to have borrowing privileges. It is understood that the PII collected is for the sole purpose of tracking and holding borrowers accountable for library materials checked out. The option to 'decline' to provide the information required to obtain borrowing privileges is not applicable in this context, as the request for borrowing privileges (requiring setup of a Patron Record) represents implicit consent for the specific uses of the PII. Use of library materials within the library may be allowed by arrangement with and at the discretion of the servicing librarian, without a Patron Record being required.

- USER ACCOUNTS (Maintenance module)
  User Accounts are limited to authorized NPS library personnel, and it is understood that the PII collected is for the sole purpose of enabling them to login into the Staff portal as an authenticated User and to access specific library operations modules and functions according to their perspective assigned permissions profiles. Their request for a Staff portal User Account, and their subsequent undertaking of required training to get their User Account activated, serves as consent for the use of their limited PII, as does the 'Accept' button at the bottom of the Security banner displayed during the Login process. A Privacy Notice is provided to the User prior to the User Account being created.

☐ 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.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and via a Privacy Notice provided to the Patron and/or the User before a Patron Record and/or User Account is created. The individuals are told why the limited PII is required, how it's used and that it's not shared beyond a select number of NPS librarians whose roles/functions warrant it. Notice is also provided through the

published DOI-58, Employee Administrative Records, SORN which may be viewed at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

There is a security banner displayed during the Login process on the staff portal.

☐ None

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

- PATRON RECORDS (Circulation module)
  - There is no explicit 'Search' feature built into the Patron Records list.
  - However, there is a Browse ('Look for') function, which enables re-sorting the displayed list of Patrons by one of the following options: Barcode (per NPS LIM policy, the NPS email address is used); first and last name (<LN, FN>); NPS email address (same content as the Barcode, but the Email field has a different function)
  - Once the 'Look for' option is selected, there is a choice of four limits that may be applied: the first is 'Browse' which is checked by default (lists all Patron Records); the other three limits (Begins With, Contains, Ends With) serve as filters (i.e., returning only a subset of Patron Records)
  - Because the system is comprised of Web pages, the Browser's 'Find on page' feature could retrieve a Patron Record by searching for a pattern contained in whatever data element has been selected for sorting the Patron Records (e.g., Barcode, which is the NPS email address, so contains first and last name of the Patron)

- USER ACCOUNTS (Maintenance module)
  - There is no 'Search' feature for User Accounts, so there is no 'retrieval' feature built into the system in that sense. However, because the system Staff portal uses Web pages, the Browser's 'Find on page' feature could retrieve a User Account by searching for PII contained as an element in the 'User Name' field (which is how the User Accounts are sorted/displayed on the page). This would be limited to first name, as only first letter of last name is used in the 'User Name' construction, whether the User is NPS staff or a Volunteer. The 'User Name' field also contains category code compound prefixes and NPS org codes, as well as library credentials, so the Browser's 'Find on a page' could be used to filter into subsets.
  - The retrieval using the Browser's 'Find on page' feature would only be effective if the first name is known. The User Accounts Manager is the only NPS LIBRIS system administrators who has the first name information.

- The 'Find on page' Browser feature cannot search within the User Account webform, so it could not retrieve on an element, such as last name, contained in an NPS email address (personal emails are not stored in User Accounts, i.e., for Users who are Volunteers)
- Locating a User Account is typically accomplished by browsing the User Accounts list, which has is alpha sorted based on the elements comprising the 'User Name'.

User Name is not the same as User Login (latter is for authentication/access control). User Name is formed via NPS LIM policy convention, which consists in all cases (with the exception of Vendor accounts, and NPS RISD system administrator and Test accounts) with the 1st element being User category compound prefix (indicating a Fed, a Partner, a Volunteer), the 2nd element being NPS org code, and the 3rd and 4th elements being first name and first letter (only) of last name, followed by any library credential, such as educational or certification information, as applicable.

I. Will reports be produced on individuals?

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

- PATRON RECORDS AND CIRCULATION REPORTS (Circulation module)
The following standard Circulation Reports include Patron Record information (Name, and/or NPS email/Patron barcode) and are run according to an automated schedule set by the librarians using the Circulation module, who may also need to run them on an as needed ad hoc basis from time to time. The use of the reports is indicated by the Report titles/descriptions, below. Nobody has access to these reports except for the few librarians authorized to use the Circulation module (controlled by the permissions profile assigned to them) and the three system administrators. However, the three system administrators have no need to run these reports, unless requested to troubleshoot. These are not technically reports 'produced on individuals,' per se -- they track library items (no Patron Records contain data on members of the public, neither do the logs):

  - Transaction Log - Items checked out for a particular period, indicating borrower (Patron)
  - List of all Circulated Items, sorted by Patron or by Title or by Borrowed Item ID#
  - List of all Overdue Items, sorted by Patron or by Title or by Borrowed Item ID#
  - List of Patrons for which borrowing privileges are scheduled to expire soon and when
  - List of Patrons for whom borrowing privileges have expired and when

  USER ACCOUNTS (Maintenance module)
  The following standard Admin Reports (located in the Maintenance module) contain Staff portal User Account information (User Login only) and are run according to a pre-set automated schedule and/or are run on an as needed ad hoc basis by the User Accounts Manager (one of the three system administrators). These are not technically reports 'produced on individuals,' per se (and User Accounts not meeting the parameters of the particular report will not be listed in the log). Nobody has access to these reports except for the system administrators, and, of these

three, only the User Accounts Manager is the one who actually runs and views the reports (System Manager is designated backup):

- Access Log: Staff portal use by Custom Login Period - Successful (default)
- Access Log: Staff portal Daily User Report (from date report is run) (default)
- Access Log: Staff portal Last 30 Days User Report (default)
- Access Log: Staff portal Last 365 Days User Report (default)
- Access Log (Columns) - Daily, Weekly, Monthly, Annually, Custom (default)
- Password Expiration
- User Record Audit Log (Columns): Daily, Weekly, Monthly, Annually, Custom
- View Active User Session
- View Current Users

☐ No

Section 3. Attributes of System Data

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

- PATRON RECORDS -- Eligible individuals requesting borrowing privileges voluntarily provide the information needed for the Patron Record to the servicing librarian, either in person or via email. It is the responsibility of the requestor to ensure accuracy of the data collected.

- USER ACCOUNTS -- Eligible individuals requesting Staff portal access voluntarily provide the information needed to create a User Account via email sent to the User Accounts Manager. It is the responsibility of the requestor to ensure accuracy of the data collected.

  The data is manually entered by the appropriate librarian to a webform template in the system. There is no automated collection of the PII. Access to the data maintained in the system is restricted to a few librarians with appropriately designated permissions as determined by role/function and NPS LIM policy. The librarian is also responsible for ensuring data entered into the webform is accurate.

B. How will data be checked for completeness?

- PATRON RECORDS -- Eligible individuals requesting borrowing privileges voluntarily provide the information needed for the Patron Record to the servicing librarian, either in person or via email. It is the responsibility of the requestor to ensure completeness of the data collected.

- USER ACCOUNTS -- Eligible individuals requesting Staff portal access voluntarily provide the information needed to create a User Account via email sent to the User Accounts Manager. It is the responsibility of the requestor to ensure completeness of the data collected.

  The librarian is responsible for ensuring the information entered into the webform is complete.

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

- PATRON RECORDS -- Eligible individuals requesting borrowing privileges voluntarily provide the information needed for the Patron Record to the servicing librarian, either in person or via email. It is the responsibility of the requestor to ensure currency of the data maintained.

- USER ACCOUNTS -- Eligible individuals requesting Staff portal access voluntarily provide the information needed to create a User Account via email sent to the User Accounts Manager. It is the responsibility of the requestor to ensure currency of the data maintained.

The librarian is responsible for ensuring the information entered into the webform 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.

All records in NPS LIBRIS that include PII are either *Temporary* (3 year retention period) or *Transitory* (retained for 180 days or less, according to NPS business requirements).

Records are covered under the NPS Consolidated Servicewide Records Schedule, Information and Public Image Management (Item 9)/NPS Records Schedule N1-79-08-8, which was approved by the National Archives and Records Administration (NARA).

1. Retention Plan. 9D. Routine and Supporting Documentation, Temporary: These records are destroyed/deleted 3 years after closure.
2. Transitory records: The retention is 180 days or less, from the date the report was generated. NPS LIBRIS Staff portal User activity and Circulation ad hoc reports are created to provide static views of operations, and are not to be retained longer than needed for business.

The records information created, captured and retained in NPS LIBRIS are routinely generated and provide documentation of those authorized to access the system and borrow library materials, and what library materials are in circulation. These records are:

- Staff portal User Accounts (approved NPS library personnel)—Temporary
- Staff portal login session activity reports (User Account PII is not included in output)--Temporary or Transitory, depending upon circumstances
- Patron Records (NPS staff requesting borrowing privileges – not used for accessing the system)—Temporary
- Circulation reports (some of which may include Patron information in the data output)--Temporary or Transitory, depending upon circumstances

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

When a Patron Record, Circulation report, Staff portal User Account, or Staff portal User activity report has served its respective functional purpose, it is deleted/purged according to Item 9.D. Retention Schedule in the NPS Consolidated Records Management Retention Schedule; or, in the case of 'Transitory' records, it is flagged for deletion after its purpose has been served and then purged within 180 days.

Any report generated in hardcopy (a rare occurrence) containing PII is stored in a locked file drawer until the end of the retention period has been reached, at which point it is shredded or pulped. Hardcopy reports not containing PII are stored in an unsecured file drawer and put in a paper recycling bin when the end of the retention period is reached.

Disposition procedures are documented in detail in the following NPS LIBRIS management documents: NPS LIBRIS SOP - User Accounts Management; NPS LIBRIS SOP - Patron Records and Circulation Reports Management.

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 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 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) 800-53r4. The system's cloud-based environment meets FedRAMP 'Moderate' (FIPS 199) security impact level compliance standards for the Infrastructure-as-a-Service (IaaS)/Platform-as-a-Service (PaaS) layers of the stack, and meets the 'Low' (FIPS 199) security impact level compliance standards for the Software-as-a-Service (SaaS) layer of the stack.

Collection, use, retention, processing, and disclosure of information is for the sole purposes of authenticating Users to the Staff portal for authorized NPS library personnel only and tracking borrowed library materials through Patron Records associated with circulated library items. Risk is mitigated by the security and privacy controls implemented to safeguard privacy. Access to data collected, stored and utilized is limited to privileged Users and authorized Contractor staff. Data is not shared outside of the system nor beyond privileged Users.

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, which are referenced in question 4.N, below, as well as in the System Security and Privacy Plans. Risk is also

mitigated through system configuration controls that limit or prevent access to privacy information and by limiting the nature and amount of PII collected from individuals and maintained in the system.

There is a risk that unauthorized Users will access the Staff portal. The system supports Single Sign-On (SSO) via PIV card/Active Directory (AD) to authenticate Staff portal Users having PIV cards ('Staff' refers to NPS library personnel). The DOI Active Directory Federation Services (ADFS) office has suspended services, so NPS LIBRIS SSO implementation is on hold. Authentication of Staff portal Users (NPS staff charged with library responsibilities and Volunteer catalogers) is via login with a User ID assigned by the User Accounts Manager combined with an encrypted Password determined by the User, in compliance with organization-defined requirements communicated to the new User and enforced by system settings that are configured by the User Accounts Manager (a system administrator).

The system uses audit logs to protect against unauthorized access, changes or use of data. All Federal employees and contractors are required to take annual mandated security, privacy and records management as well as role-based training where applicable and sign the 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 individuals providing information may not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA, the privacy notice provided to patrons and users in person, and the DOI-58, Employee Administrative Records, SORN. NPS employees are provided privacy notice and voluntarily submit their name and official email address to create a Patron account in order to borrow library items. Employees may update or correct their account information at any time by contacting the librarian.

There is a risk that information in the system will be retained longer than necessary to achieve the agency's mission or will be deleted prematurely. This risk is mitigated by maintaining and disposing of the User Accounts, associated User activity reports, Patron Records and Circulation reports in accordance with the NPS Consolidated Records Management Retention Schedule N1-79-08-8. Detailed retention and disposition procedures are documented in the following NPS LIBRIS management documents: NPS LIBRIS SOP - User Accounts Management; NPS LIBRIS SOP - Patron Records and Circulation Reports Management.

Risk at all phases of the information lifecycle is mitigated by compliance with security and privacy controls required by NIST SP 800-53, with DOI enhancements, which are reviewed annually (one third of the controls per year) for the three years following issuance of the Authority to Operate.

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 System is designed to support library collections management activities, including System Administration, Cataloging and Circulation, which require Staff portal User Accounts and Patron records for Borrowers. Borrowers are limited to NPS staff and Patron records are not used to access the system, only to track circulated 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?

Not applicable. 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(s) [NOTE: also referred to as 'Privileged Users']
☐ Other:

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 of the NPS LIBRIS Staff portal and limited to authorized NPS library personnel, except for the System Administrators, who have full privileges.

- Each Staff portal User Account will be assigned a permissions group number; groups of permissions are used to define a User's category (role).

- The permissions will determine which modules the User may access and what functions within those modules they may execute in the System and define what records the User can view, create, edit and delete, and what library management operations reports they can run and view.

- System management staff may view PII in the performance of their duties for routine processes (e.g., User Accounts management), occasional system maintenance purposes or troubleshooting.

- Privileged Users are subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

All required Privacy Act contract clauses are included in the annual Period of Performance (PoP) beginning 04/20/2021 -- in accordance with and subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a)

☐ 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*

- Monitoring will primarily target Staff portal Users with privileged accounts, such as System Administrators who can change System configuration settings and elevate access roles or permissions; however, login history is recorded for all Users, and field history tracking is recorded for select data fields, including PII data such as unique identifier and NPS org code signifying the NPS work unit for which the User is performing activities in the System (i.e., their 'work location')

- NPS LIBRIS is not intended for locating and monitoring individuals, per se; however, the System does identify and monitor User activities in the System through audit logs; these audit logs automatically collect and store information about a Staff portal User's Logon session, including unique identifier, identify verification method, action attempted and status of attempt (i.e., whether successful or unsuccessful)

- In addition, the System collects and stores administrative metadata related to library collections management activities performed by Staff portal Users to support User access controls, troubleshooting, and incident response support, as well as to track changes to library metadata that are routine but key data points.

- 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?

- The System logs all system access and internal processes, including monitoring, maintenance and audit processes. Data elements logged include User Account unique identifier, timestamp, event, source and successful/unsuccessful login attempts.

- System Administrators have full privilege access to the User Accounts Setup area and to the Admin Reports area. When run, these reports output information automatically stored in the System's internal monitoring logs. System Administrator User Accounts are monitored and routinely audited.

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

- System Administrators -- as with all NPS staff -- are required to take annual Role-Based Security Training (RBST), annual Role-based Privacy Training (RBPT), and annual Information Management Training including security, privacy, records management, and Controlled Unclassified Information.

- System Administrators -- as with any User of the NPS LIBRIS Staff portal (which is for authorized NPS library personnel only, including NPS LIBRIS system administrators) -- must 'Accept' the DOI system usage statement before access to the system is enabled.

- Separation of duties, permissions restrictions and audit controls are implemented to prevent unauthorized monitoring; only System Administrators have access to the User Accounts area, the Admin Reports area, and monitoring log files.

- Established procedures control the granting of User Accounts, and privileged accounts are routinely audited for compliance.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Biometrics
☒ Intrusion Detection System (IDS)
☒Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The NPS Resource Information Services Division (RISD) Chief is the designated Information System Owner and is responsible, along with the Information System Security Officer (ISSO) assigned to NPS LIBRIS, 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 NPS LIBRIS, in consultation with NPS Associate Privacy Officer and DOI Privacy Office.

As the Information System is a Software-as-a-Service (SaaS) application, the Contractor also has responsibility for protecting privacy rights and the information maintained in the system.

The NPS LIM program manager/team leader, and one of three NPS LIBRIS System Administrators, is the designated NPS LIBRIS System Manager and, as such, is responsible for oversight and management of the security and privacy controls, the protection of information processed and stored in NPS LIBRIS, and reporting to the Information System Owner any Privacy Act complaints and requests for redress or amendment of records.

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 Information System Owner and the ISSO 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.

The NPS LIBRIS System Manager is responsible for daily operational oversight and management of the security and privacy controls, and for ensuring to the greatest possible extent that data is properly managed and that access to the data has been granted in a secure and auditable manner.

All Users of the NPS LIBRIS Staff portal, librarians, System Administrator, and System Managers are required to report any potential loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.

As the Information System is a SaaS, the Contractor shares responsibility with NPS for assuring proper use of the data, per their FedRAMP authorization requirements and is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information to the NPS LIBRIS System Manager.