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: ExLibris Integrated Library System
Bureau/Office: U.S. Geological Survey (USGS), Core Science Systems (CSS)
Date: December 14, 2022
Point of Contact:
Name: Cozenja M. Berry
Title: Associate Privacy Officer
Email: privacy@usgs.gov
Phone: 571-455-2415
Address: 12201 Sunrise Valley Drive, Mail Stop159, Reston, VA 20192

Section 1. General System Information

A. Is a full PIA required?

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

☐ No

B. What is the purpose of the system?

The U.S. Geological Survey (USGS) procured ExLibris as a Software As A Service (SaaS) in support of the USGS Library mission. The USGS Library is a component of the Science Analytics and Synthesis (SAS) program under the Core Science Systems (CSS) Mission Area. The USGS Library is a multisite, centralized library, providing bureau-wide access to scholarly journals and research support services to USGS personnel around the nation. On site library operations are in Reston, Virginia; Denver, Colorado; and Menlo Park, California. An important

role of the USGS Library is the preservation of its unique physical collections, ensuring continued access for future generations. The USGS Library is recognized as one of the world's largest Earth and natural science libraries, providing services, collections, and expertise that are essential to the USGS mission and the global geoscience community. The library's online catalog is a public interface to its bibliographic database which contains over 350,000 records of item holdings/inventory of materials in many different formats, including books, maps, manuscripts microfilm, and digital media. The ExLibris system is designed specifically for large libraries with specialized collections (i.e., government, nonprofit, legal, and medical).

The purpose of ExLibris is to provide an integrated library system (ILS) to support highly efficient library collections management and search/discovery processes benefiting the USGS library staff and library users. It enables USGS library staff to perform collaborative cataloging using a central suite of integrated modules and provides library users with fast and sophisticated public catalog search and discovery features for determining and locating relevant resources. The public-facing, read-only catalog of records in ExLibris are made available by USGS through the Online Computer Library Center (OCLC), a national bibliographic utility that facilitates Inter-Library Lending (ILL) and borrowing transactions. The USGS Library uses the OCLC to borrow materials on behalf of USGS personnel and loan its library holdings to members of the general public via their local library (i.e., public, school, university, or corporate library).

The following individuals may benefit from the services available through ExLibris as USGS library users:

-    Other librarians. Particularly DOI librarians, as some USGS scientific holdings are multiagency or are otherwise relevant to one or more DOI bureaus and offices.

-    USGS personnel and affiliates. The following individuals are eligible to establish library patron accounts: full-time and part-time permanent USGS employees; temporary USGS employees; USGS Scientists Emeritus; contractors working for USGS; and volunteers and interns with USGS credentials. USGS individuals who register for a library patron account are granted borrowing privileges and access to available on-line subscription services (journals, newspapers, and other digitized services). Links in the library catalog route through a proxy server to authenticate users against the DOI Active Directory before connecting to subscribed content. ExLibris enables registered library patrons to request library materials, initiate interlibrary loans, manage their borrowing accounts, and access subscribed electronic journal content (USGS personnel and affiliates only).

 - Members of the general public. Members of the general public who are not affiliated with the USGS may conduct research on-line as a guest or visit the USGS library in person. Visitors may use library materials on the premises during normal operating hours. As a requirement for entry to a Federal building, a government-issued identification must be presented to access USGS library facilities. Visitors must comply with facility security procedures which may include security screening, building sign-in/out logs, and badging. To borrow materials from the USGS library, members of the public must ask their local library to submit their request through either the OCLC electronic ILL system or on the standard American Library

Association (ALA) form by email, mail or FAX to the appropriate library location. The USGS library does not receive any personal information on individuals who borrow materials via the ILL. Lastly, individuals may seek information or assistance through the "Ask a Librarian" email. Email communications with library staff are maintained in accordance with Federal records laws and will be handled as required by the Privacy Act and the Freedom of Information Act to ensure the greatest protection of personal privacy.

C. What is the legal authority?

5 U.S.C. 301, Departmental Regulations; 20 USC 91: Literary and scientific collections accessible to investigators and students; 43 U.S.C. 1457: Duties of Secretary; 43 U.S.C. 31, Director of United States Geological Survey; 43 USC 36: Purchase of books; 43 U.S.C. 36a: Acquisition of scientific or technical books, maps, etc., for library; 43 USC 41: Publications and reports; preparation and sale.

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: Asset 434 Integrated Library System

☐ No

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

Subsystem Name	Purpose	Contains PII (Yes/No)	Describe If Yes, provide a description.
None			

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

☒ Yes. 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

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Gender
☒ Birth Date
☒ Other:

Library Patron Records. These records are limited to USGS personnel and eligible affiliates (full-time and part-time permanent USGS employees; temporary USGS employees; USGS Scientists Emeritus; contractors working for USGS; and volunteers and interns with USGS credentials) who register for patron accounts. Required PII elements include: first name, last name, USGS email address, office mailing address, affiliated area or office, and a unique system assigned primary identifier number. Active Directory credentials are used to access individual accounts and subscription services. Middle name, gender, preferred name, and date of birth are optional fields that are not used or required by the USGS. 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 general public who are not affiliated with the USGS are not extended borrowing privileges, and therefore patron records are not maintained for them. The library creates borrowing records to facilitate check-out transactions to external institutions through Interlibrary Loan. This information includes the institution name, OCLC code, and mailing address.

Library Staff User Accounts. For authorized library personnel, PII collected includes Active Directory information to include first name, last name, USGS email address and affiliated area or office. Individuals approved to perform library collections management and processes via the USGS ExLibris Staff portal voluntarily provide their PII to the user account manager. These users require user login and password to access the staff portal. Access to user account PII is restricted to system administrators with permissions to the maintenance module.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ DOI Records

PII is collected from the individual and DOI Active Directory.

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

☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Information Shared Between Systems

Individuals who establish library patron accounts may provide PII online, in person, or via email. Individuals who require library staff user accounts may provide PII via email. ExLibris interfaces with DOI Active Directory to authenticate USGS personnel credentials.

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

Library Patron Records. 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.

Library Staff User Accounts.   PII collected is used to securely authenticate individuals to the system's staff portal, manage staff user account 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:

Library Patron Records. System administrators and servicing librarians have access to patron records. The servicing librarians access patron records for routine purposes to include creating, updating, or flagging patron records for deletion. The system administrators have a periodic need to access patron records for auditing and to ensure compliance with required security controls.

Library Staff User Accounts. System administrators have access to staff user account records. The system administrator assigned to the User Account Manager role accesses this area on a regular basis to set-up new accounts, delete accounts, and reset passwords. The system administrators have a periodic need to access user account records for auditing and to ensure compliance with required security controls.

☒ Contractor: 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 ExLibris application. The Contractor provides licensing, hosting, maintenance, monitoring, system support and 24-7 Client support services. The required Federal Acquisition Regulation (FAR) clauses for compliance with the Privacy Act of 1974 (as amended) are included in contracts.

Additional disclosures may be permitted only when consistent with the purpose of the activity and the uses are authorized under the Privacy Act and as stated in the routine uses in the system of records notice, DOI-58, Employee Administrative Records.

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

☒ Yes.

Library Patron Records. USGS personnel and eligible affiliates may choose to establish a library patron account. It is understood that the PII collected is for the sole purpose of tracking library materials and holding borrowers accountable for items 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 represents implicit consent for the specific uses of the PII.

Library Staff User Accounts. User accounts are limited to authorized USGS library staff. It is understood that the PII collected is for the sole purpose of enabling them to login the staff portal as an authenticated user and to access specific operations modules and functions according to role based permissions. The individual request for a staff user account, and completion of required training, serves as consent for the limited use of their PII, as does the 'Accept' button at the security banner displayed during the login process. In addition, a privacy notice is provided to the user prior to the user account being created.

☐ No

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

☒ Privacy Notice: Notice is provided through publication of this PIA and via a privacy notice provided to the individual before their patron record or user account is created. Notice is also provided through the published DOI-58, Employee Administrative Records, system of records notice which may be viewed at https://www.doi.gov/privacy/sorn. Further, the customer has access to information provided in the following link, which details information on the USGS web privacy policies at https://www.usgs.gov/privacy-policies.

☒ Other: There is a security banner displayed during the login process on the staff portal.

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

Library Patron Records and Library Staff User Accounts may be retrieved by individual's name or email address.

I. Will reports be produced on individuals?

☒ Yes. Reports may be generated for patron records to provide a list of borrowed, overdue, and wait-list library materials. Library patron's name and email address may be included on the reports. Reports are temporary and run on an as-needed basis to manage and account for library materials. Access is restricted to library staff as it pertains to their assigned duties and responsibilities.

☐ No

Section 3. Attributes of System Data

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

Library patrons and library staff provide their PII and therefore are responsible for verifying the accuracy of their PII data on submission. Name and email addresses may be authenticated through the DOI Active Directory to verify the individual is eligible to establish a library patron account. PII submitted for library staff user accounts is verified via DOI records by system administrators before accounts are established.

B. How will data be checked for completeness?

Library patrons and library staff provide their PII and therefore are responsible for verifying the completeness of data. There are mandatory fields (first name, last name, USGS email address, physical address, affiliated area or office) that must be completed by the individual.

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

Library patrons and library staff must ensure their information remains current. Library patrons can update their account information. Patron accounts are disabled when individuals leave the agency via the 9090 Form USGS Exit process. Library staff user accounts are disabled when the individual no longer requires access to perform the associated duties. Procedures are documented in library business procedures.

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

Library patron records are retained in accordance with the USGS General Records Disposition Schedule (GRDS). The applicable GRDS is 306-10c, Library administrative records, which includes records documenting library planning and management, policies, procedures, and statistics. These records have a temporary disposition and are destroyed when 3 years old or 3 years after superseded or obsolete, whichever is applicable. Longer retention is authorized for business use.

Library Staff User Accounts are retained in accordance with the USGS General Records Disposition Schedule (GRDS). The applicable GRDS 204-11, System Access Records, which includes records created as part of the user identification and authorization process to gain access to systems. These records have a temporary disposition and are destroyed when the business use ceases.

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

Paper records are shredded in accordance with records retention guidelines. Electronic records are deleted. Backup tapes are reinitialized and reused. Approved disposition methods include erasing, degaussing, deleting, and shredding in accordance with the appropriate records schedule, DOI records policy, and National Archives and Records Administration (NARA) guidelines.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a minimal risk to individual privacy as ExLibris only collects non-sensitive PII on library patrons and library staff users. Collection, use, retention, processing, and disclosure of PII is for the sole purposes of authenticating access to ExLibris and tracking borrowed library materials through patron records associated with circulated library items. ExLibris is rated as a FISMA moderate system and requires management, operational, and technical controls established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 to mitigate the privacy risks for unauthorized access, disclosure, misuse of PII, and malicious attacks. The risks are mitigated through administrative, physical, and technical controls that have been implemented to protect the confidentiality, integrity, and availability of information in the system. The ExLibris Library system is in use across thousands of Libraries throughout the world.

There is a risk of unauthorized access to the system or data. Security controls have been implemented to prevent unauthorized access to patron records throughout the information lifecycle. Platform and device level encryption have been deployed to encrypt data at rest. Audit Logs are kept on all system activity with tools in place to look for abnormal activity and intrusion detection. Other system security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection tools.

There is a risk for inappropriate use, or disclosure of information to unauthorized recipients. To mitigate this risk, the USGS Library follows the least privilege security principle and strictly limits access to library patron data based on an official need to know. Access to records in ExLibris is limited to authorized library staff who have a need to access the records in the performance of their official duties. Data is not shared outside of the system nor beyond privileged users. Additionally, patron data is only used for the purposes as specified in this PIA and the associated system of records notice. System administrators and authorized users are trained and required to follow established internal security protocols. All library staff users must complete records management, Paperwork Reduction Act (PRA), Section 508, Controlled Unclassified Information (CUI), and role based privacy training on an annual basis. Moreover, they must review and agree to the DOI Rules of Behavior.

There is a risk that individuals may not receive adequate notice of the purposes for collecting their personal information in ExLibris or whom the information may be shared with. Library patrons are provided privacy notice and voluntarily submit their name and official email address to create a patron account in order to borrow library items. Patrons may update or correct their account information at any time by contacting the librarian. Individuals are notified of the privacy practices through published DOI SORNs, privacy notice, and the USGS website privacy policy. This PIA also provides a detailed description of ExLibris data elements, uses of personal information, and how customer PII is shared.

There is a risk that information in the system will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The ExLibris system owner will ensure that the identified records are maintained and disposed of in accordance with records retention schedules that were approved by NARA. Library staff users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Library patron records regardless of media (paper or electronic) are safeguarded in accordance with applicable laws, rules and policies.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes. The system is designed to support library collections management activities, including system administration, cataloging and circulation, which require library staff users and patron records for borrowers. Borrowers are limited to USGS 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

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes

☒ No

E. How will the new data be verified for relevance and accuracy?

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.

☐ Yes, processes are being consolidated.

☒ No, data or processes are not being consolidated.

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

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other:

Library patrons (may include USGS contractors) only have access their own PII stored in their patron record. Library patrons do not have access to other individuals PII or account information. Members of the general public not affiliated with the USGS are not authorized to establish library patron accounts, therefore they have no access to PII maintained in the system.

Library staff users/system administrators, typically less than 4 individuals across all Library locations, (may include USGS contractors) require a DOI Active Directory account and must have need-to-know in order to perform their official duties. The system may only be accessed from within the DOI network or using the DOI Virtual Private Network (VPN).

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

Library patrons' access is restricted to their own account registration information and borrowing history. Patrons do not have access to other individuals PII or account information.

Library staff user access to ExLibris is determined by functional responsibilities. Staff users must complete a system authorization access request. System Administers work with supervisors to define user roles, change permissions, and remove access as needed.

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. Privacy Act contract clauses are included in all contracts. Contractors must sign a non-disclosure agreement upon employment and are required to complete annual privacy and information security training.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes

☒ No

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

☒ Yes. User monitoring is limited to information provided in system and web logs for system security administration purposes only.

☐ No

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

IT audit logs include username, hostname, logon dates, times of failed logon attempts, IP addresses, webpages accessed, processes accessed and other system failures.

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

The use of USGS IT systems is conducted in accordance with the appropriate use policy. As ExLibris is a SaaS, the contractor (service provider) shares responsibility with USGS for preventing unauthorized monitoring, per their FedRAMP authorization requirements. The system maintains an audit trail of activity sufficient to reconstruct security-relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis, and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Further, system access for USGS library staff users is determined by functional responsibilities. Users consent to monitoring when accessing government maintained systems. In addition, use of personally owned equipment is prohibited; government furnished equipment must be used to access the system. Users are required to complete a system authorization access request, which must be signed by their supervisor. USGS personnel with system administrator access must complete IT security and privacy awareness training as well as role-based training before being granted access to the system, when required by system changes, and at least annually thereafter.

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

(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

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

The Deputy Director, Science Analytics and Synthesis (SAS), is the ExLibris System Owner and the official responsible for oversight and management of ExLibris security and privacy controls, including the protection of information processed and stored by ExLibris. The System Owner is also designated as the Privacy Act system manager and is responsible for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system of records, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the USGS Associate Privacy Officer (APO). Specific guidance on how DOI implements the Privacy Act has been published to the Code of Federal Regulations at 43 CFR Part 2, Subpart K.

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 ExLibris System Owner is responsible for oversight and management of the system security and privacy controls and for ensuring, to the greatest possible extent, that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team and DOI Computer Incident Response Center immediately upon discovery in accordance with Federal policy and established procedures. Incidents involving PII must be reported to the USGS

APO and are managed in accordance with procedures outlined in the DOI Privacy Breach Response Plan. The APO oversees breach reporting and response activities to include incident investigation, mitigation efforts, and implementing corrective actions following a breach.