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: Laserfiche Document Management System (LDMS) Decommissioning
Bureau/Office: Office of the Secretary
Date: December 19, 2018
Point of Contact:
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

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 Laserfische Document Management System (LDMS) was managed by the Office of the Chief Information Officer (OCIO) and consisted of the following databases:

Document Management Unit (DMU) Database
The DMU Database manages the process by which DOI responds to requests for production of documents by the courts and Congress, compiles Administrative Records for the Office of the Solicitor, and creates other document collections. The DMU Database is capable of scoping and defining document searches; controlling the manner in which collected documents are submitted to the system, imaged, and coded; organizing document collections for future review; and producing selected documents using a variety of search criteria. Both electronic and paper documents may be submitted to the DMU for storage and indexing. Paper documents were electronically scanned and processed with optical character recognition software to add machine readable text to the scanned image file. As a result, the majority of documents uploaded to the DMU Database are fully searchable by keyword. The DMU Database may be used to collect documents or data of any type held by DOI, including documents that may contain personally identifiable information (PII). It is expected that significant amounts of PII are collected from DOI employees and members of the public because of the expansive scope of the DMU Database and the document collections it hold.

Electronic Library of Interior Policies System (ELIPS)
ELIPS serves as the Department's repository of official policies, procedures, and programs. ELIPS contains copies of policy documents and guidance memoranda that include the name, title and signature of one or more DOI officials. In some cases, ELIPS documents may include name and business contact information of DOI employees. The ELIPS database does not include sensitive PII.

Office of Surface and Mining Database (OSM Database)
The OSM Database stores documents and correspondence related to OSM's business functions, including project support, permitting, maps, and mining data. The majority of documents in the OSM Database are technical and regulatory in nature, and will not contain PII; however, it collects a moderate amount of PII from OSM employees, other DOI bureaus and offices, Federal agencies, and state and local officials with any involvement in mining activities. The OSM Database may also contain PII of members of the public such as the names and addresses of private landowners who own property abutting surface mines, or the names of individuals who provide comments regarding specific mining operations or mining permits.

Office of the Chief Information Officer Database (OCIO Database)
The OCIO Database contains administrative memorandums and directives related to IT Transformation, which involved restructuring DOI's information technology staffing to better align information technology capabilities with DOI's business and mission areas while reducing overall IT spending.

Office of Inspector General Database (OIG Database)
The OIG Database provides case file management for OIG, including serving as a repository for case histories, notes, and contact information related to audits, inspections, and civil and criminal investigations. The OIG Database stores a moderate amount of PII, such as name, title and contact information of OIG and DOI current and former employees and contractors. Some OIG case files may also contain PII of other Federal employees, state and local government employees, individuals from Indian tribes, or other members of the general public.

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS were removed from the network, and are no longer operational. A decommissioning plan was completed for LDMS to outline and document the decommissioning procedures, and ensure the system was decommissioned in a secure and auditable manner. The data owners of the organizations identified above are responsible for ensuring data was properly migrated, stored, and disposed of in accordance with the approved records schedule.

The OSM, OCIO, and OIG databases have been taken offline and decommissioned. Data was disposed of in accordance with the approved records disposition procedures, or preserved at different locations for records that are still being maintained.

The DMU Database has been replaced by Advanced Early Case Assessment (AECA) within the eMail Enterprise Records and Document Management System (eERDMS), DOI's framework for using, storing, accessing, and managing records; however, no data was migrated to AECA. The DMU legacy data were disposed of in accordance with the records schedule. Data required to be maintained were backed up on disks and stored by the Office of the Executive Secretariat (OES).

ELIPS was replaced with Drupal on DOI.gov. Legacy data was stored on the OCIO shared drive and Google Drive within the BisonConnect environment. ELIPS data was migrated to Drupal and verified by document owners.

C. What is the legal authority?

Departmental Regulations, 5 USC 301; The Paperwork Reduction Act,44 U.S.C. Chapter 35; The Government Paperwork Elimination Act, 44U.S.C. 3504; the Clinger-Cohen Act, 40 U.S.C. 1401; Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service*, April 11, 2011; and OMB Circular A-130, *Managing Information as a Strategic Resource*.

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*:

010-000000701; Laserfiche Document Management System (LDMS) System Security Plan

☐ No

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

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

The OCIO, OIG, and OSM databases within LDMS are covered by the following SORNs.

- DOI-45, HSPD-12: Identity Management System and Personnel Security Files, 72 FR 11036 (March 12, 2007)
- OIG-1, Management Information, 55 FR 14480 (April 18, 1990)
- OIG-2, Investigative Records, 76 FR 60519, (September 29, 2011)
- OSM-8, Employment and Financial Interest Statements - States and Other Federal Agencies, 64 FR 17412 (April 9, 1999); modification published at 73 FR 45244 (August 4, 2008)
- OSM-12, Blaster Certification, 64 FR 17412 (April 9, 1999); modification published at 73 FR 45244 (August 4, 2008)

These notices may be viewed on the DOI SORN website at http://www.doi.gov/privacy/sorn.

☐ 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.

☒ Other: *Specify the PII collected.*

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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*

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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

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

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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

LDMS was decommissioned and is no longer used to collect or maintain PII. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. Please see the eERDMS PIA on how data is collected and used by AECA within eERDMS. ELIPS data was migrated to Drupal on DOI.gov.

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.*

LDMS was decommissioned and is no longer used to collect or maintain PII. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. Please see the eERDMS PIA on how data is managed and shared in AECA. ELIPS data was migrated to Drupal on DOI.gov.

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

LDMS was decommissioned and is no longer used to collect or maintain PII. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. Please see the eERDMS PIA on how data is managed and shared in AECA. ELIPS data was migrated to Drupal on DOI.gov.

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

LDMS was decommissioned and is no longer used to collect or maintain PII. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. Please see the eERDMS PIA on how data is managed and shared in AECA. ELIPS data was migrated to Drupal on DOI.gov.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

LDMS was decommissioned and is no longer used to collect or maintain PII. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. Please see the eERDMS PIA on how data is managed and shared in AECA. ELIPS data was migrated to Drupal on DOI.gov.

☒ Contractor: *Describe the contractor and how the data will be used.*

LDMS was decommissioned and is no longer used to collect or maintain PII. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. Please see the eERDMS PIA on how data is managed and shared in AECA. ELIPS data was migrated to Drupal on DOI.gov.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

LDMS was decommissioned and is no longer used to collect or maintain PII. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. Please see the eERDMS PIA on how data is managed and shared in AECA. ELIPS data was migrated to Drupal on DOI.gov.

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.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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.*

☐ 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.).

Not applicable. LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

J. 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?

Not applicable. LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

B. How will data be checked for completeness?

Not applicable. LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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

Not applicable. LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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

LDMS was decommissioned and records were disposed of in accordance with the applicable Departmental records retention schedule, Departmental policy and NARA guidelines. The data within the OSM, OCIO, and OIG databases were disposed of in accordance with the approved records disposition procedures, and preserved at different locations for records that are still being maintained. The DMU legacy data were disposed of in accordance with the records schedule, data backed up on disks are stored by OES. ELIPS data was migrated to Drupal.

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

LDMS was decommissioned and records were disposed of in accordance with the applicable Departmental or bureau/office records retention schedule, Departmental policy, and NARA guidelines. Paper records were disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with 384 Department Manual 1.

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 limited privacy risk for the decommissioning of the LDMS system. LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS were removed from the network, and are no longer operational. A decommissioning plan was completed for LDMS to outline and document the decommissioning procedures, and ensure the system was decommissioned in a secure and auditable manner. The data owners of the organizations identified above are responsible for ensuring data was properly migrated, stored, and disposed of in accordance with the approved records schedule.

The OSM, OCIO, and OIG databases have been taken offline and decommissioned. Data was disposed of in accordance with the approved records disposition procedures, and preserved at different locations for records that are still being maintained. The DMU Database has been replaced by AECA within eERDMS; however, no data was migrated to AECA. The DMU legacy data were disposed of in accordance with the records schedule. Data backed up on disks are stored by OES. ELIPS was replaced with Drupal on DOI.gov. Legacy data was stored on the OCIO shared drive and Google Drive within the BisonConnect environment. ELIPS data was migrated to Drupal and verified by document owners. After the hardware was decommissioned, LDMS data was archived onto backup tapes and disks and stored by OCIO Hosting Services. DOI has implemented adequate physical, technical, and administrative controls to protect the data from unauthorized access or disclosure. Data stored on backup tapes and disks are located at secure DOI facilities.

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*
☒ 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?

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline

and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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*

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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?*

☒ 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*
☒ No

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

Not applicable as LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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

Not applicable as LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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 *(in Google Drive)*
☒ Identification Badges
☒ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe*

LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. Data that are still being maintained are stored in a secure DOI facility.

(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*

LDMS was decommissioned and is no longer used to collect or maintain PII. There are technical controls in place to protect data that was migrated or still being maintained in other DOI systems, including firewall, IDS, and VPN. Please see the eERDMS PIA for technical controls for DMU data, and the Drupal PIA for ELIPS data.

(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*

LDMS was decommissioned and is no longer used to collect or maintain PII. There are administrative controls in place to protect data that was migrated or is still being maintained, including 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. Please see the eERDMS PIA for administrative controls for DMU data, and the Drupal PIA for ELIPS data.

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 Departmental Records Officer is the LDMS System Owner responsible for oversight and management of security and privacy controls of data processed and stored by LDMS. The LDMS System Owner is also responsible for ensuring adequate safeguards are implemented to protect privacy in compliance with Federal laws and policies for the data retired and disposed of in LDMS, in consultation with the DOI Privacy Officials. LDMS was decommissioned and is no longer used to collect or maintain PII. The databases within LDMS are not operational. The OSM, OCIO, and OIG databases have been taken offline and decommissioned. The DMU Database has been replaced by AECA, and legacy data are stored by OES. ELIPS data was migrated to Drupal on DOI.gov.

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 LDMS System Owner is responsible for daily operational oversight and management of the LDMS system and for ensuring to the greatest possible extent that security and privacy controls are implemented to properly manage and safeguard data for the data retired and disposed of in LDMS in collaboration with the offices who are the data owners. The LDMS System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and the DOI Privacy Office in accordance with Federal policy and established DOI breach response policy and procedures.