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: Legal Hold Pro System (LHP)
Bureau/Office: Office of the Solicitor
Date: September 30, 2021

Point of Contact
Name: Danna Mingo
Title: Departmental Offices Associate Privacy Officer
Email: OS_Privacy@ios.doi.gov
Phone: (202) 441-5504
Address: 1849 C Street NW, Mail stop 7112 MIB, 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:

B. What is the purpose of the system?

Legal Hold Pro (LHP) is an approved LLC cloud-based Software as a Service (SaaS) automated legal hold distribution and tracking system. The system is designed to enable the Department of the Interior (DOI) Office of the Solicitor (SOL) to quickly issue and effectively manage legal holds via a combination of automatic and simplified workflows.

The United States' judicial system is firmly rooted on the belief that parties to litigation should share documents and other information prior to trial. In support of that proposition, each party has a duty to the court to identify, locate, and preserve information and other evidence that is relevant to the claims and defenses at issue in litigation. The parties must take reasonable steps to avoid the intentional or inadvertent destruction or loss of relevant evidence that might be used at trial. LHP is an important component of SOL's comprehensive data preservation and electronic discovery program and helps Departmental stakeholders meet their important information legal preservation obligations. SOL intends to integrate LHP with the Department's existing eMail, Enterprise Records, and Document Management System (eERDMS) to ensure records subject to legal holds are preserved.

C. What is the legal authority?

43 U.S.C. 1455

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: 010-000002389 Legal Hold Pro
☐ 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	Describe
None			

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

☒ Yes:

SOL-01, Litigation, Appeal and Case Files, 46 FR 12150, February 12, 1981, which may be viewed at: https://www.doi.gov/privacy/sol-notices. This notice is currently being revised and will be published in the Federal Register.

☐ 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
☒ Personal Email Address
☒ Other Names Used
☒ Other:

Official email addresses are used to generate notifications of legal holds to records custodians and to track the records custodians' acknowledgement of their receipt and understanding of their obligation to preserve records subject to a legal hold. SOL may possibly use an individual's personal email address when, in the normal course of litigation, it becomes apparent that the individual has used their personal email address to conduct official business related to a specific legal matter.

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

☐ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source

☐ State agency
☐ Other: *Describe*

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

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

Department employees and contractors will manually access and copy information from the BisonConnect Contacts database and the DOI-Access database to populate names and email addresses of legal hold notice recipients. (Names and email addresses are manually entered into https://www.legalholdpro.com Legal Hold Pro.)

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

The names and email addresses of Department employees and contractors will be used to track personnel subject to legal holds, to distribute the necessary notices to those individuals, and to track their responses to interview questions regarding the information in their custody which may be relevant to a specific legal matter.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office:

SOL will use the PII to send notifications and track legal hold custodians' compliance with their preservation obligations.

☒ Other Bureaus/Offices:

Other bureaus and offices will be given periodic reports from the system to enable them to directly track the preservation efforts of custodians in each bureau or office.

☒Other Federal Agencies:

Data will be shared with the Department of Justice so that it can be used as evidence of the Department's information preservation efforts, and with other Federal agencies as authorized under other routine uses outlined in the SOL-1, Litigation, Appeal and Case Files SORN, which may be viewed at https://www.doi.gov/privacy/sol-notices.

☒ Tribal, State or Local Agencies:

Information may be shared with state, territorial and local governments as necessary and proper, when there is a subject matter interest in the records and the disclosure is compatible with the purpose for which the records were compiled.

☒ Contractor:

The Department has an annual service sub-contract with the vendor of the Legal Hold Pro cloud-based database system, Zapproved. The vendor's system administrators are expected to perform routine system maintenance and will have no business reason or authority to access the PII in the conduct of their official duties on behalf of the Department. Departmental contractors who provide support to SOL related to litigation or preservation matters may have access to PII to perform their assigned duties.

☐ Other Third-Party Sources:

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

☐ Yes:

☒ No:

Employee names and official email addresses are retrieved from existing DOI records for the purpose of generating notification emails to records custodians, and employees are not provided an opportunity to consent to the use of their name and email address for this purpose. Department employees and contractors are responsible for complying with their preservation obligations and communicating with SOL regarding any potentially relevant information in their custody.

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

☐ Privacy Act Statement:

☒ Privacy Notice:

Privacy notice is provided through the publication of this privacy impact assessment and the published SOL-1 Litigation, Appeal and Case Files system of records notice, which may be viewed at: https://www.doi.gov/ocio/policy-mgmt-support/privacy/SOL-1-Litigation-Appeal-Case-File.

☐ Other: *Describe each applicable format.*

☒ None

Department employees and contractors are generally not asked to provide sensitive PII data.

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

Data will be retrieved from the system by case name, case number, or matter name.

I. Will reports be produced on individuals?

☒ Yes:

Reports will be used to track the compliance and responses of legal hold custodians. Only a small number of system administrators and the attorneys and staff members assigned to each matter will have access to these reports.

☐ No

Section 3. Attributes of System Data

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

Not applicable

B. How will data be checked for completeness?

The PII stored by the system will be obtained from reliable, existing DOI records.

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

The names and email addresses of custodians will be updated as they are identified as being subject to newly implemented legal holds. Custodians' names and email addresses

will also be updated upon the discovery of any failure of email communications between the Office of the Solicitor and the custodians.

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

Data within the system has a temporary retention per DAA-0048-0018-0002, item 0017, Legal Compliance and Reporting (awaiting approval by NARA as of January 2021, but in final review stage). Data is cut off at the end of the fiscal year in which the subject matter is closed, or after the document creation date, if closure does not apply. The data is destroyed six (6) years after cut-off.

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

Upon the closure of a hold, audit logs are exported and stored in the Department's Enterprise Content Server (ECS) database. The logs are retained according to the GRS and dispositioned at the end of their Federal records retention period. Data within the system that has met its retention will be purged, in accordance with instructions on the DI 1941 form, completed by Solicitor's office and authorized by the Office of the Secretary Records Management office. Additional information is available in Departmental Manual DM 380, and RMP-2020-03 Records Disposal Authorization (draft as of January 2021).

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 minimal risk to privacy as the user information consists of name and official email address that are not considered sensitive PII. The Department employees and contractors who are identified as potential custodians of information potentially relevant to litigation involving the Department do not have a discernible privacy interest in their names and official email addresses being included on a list of individuals who may have information that is potentially relevant to a particular legal matter.

There is a risk that DOI will collect more information than is necessary. This risk is mitigated by only using the minimal amount of information necessary to effectively meet requirements to track litigation holds and meet Departmental needs. There is a risk of maintaining inaccurate information that may result in incorrect determinations. This risk is mitigated through established procedures to verify correct information for records custodians.

There is a risk that unauthorized individuals may access the information in LHP or use it for an unauthorized purpose. This risk is mitigated by ensuring effective access controls

are implemented, and only authorized personnel are granted access to LHP, and users agree to adhere to the DOI Rules of Behavior.

There is also a risk that information in LHP may be used outside the scope of the purpose for which it was collected. This risk is mitigated by the access controls implemented to ensure only authorized personnel have access to the records needed to perform official duties, and these users complete role-based privacy training every year in addition to the annual Privacy Awareness training. Disclosure of data to other agencies and organizations is in accordance with the published SOL-1 system of records notice and is subject to all applicable Federal laws and regulations. Data within the system which may contain PII is protected during destruction following approved DOI and NARA guidelines.

There is a risk that some data may not be appropriate to transfer or store in vendor cloud-based solutions, or that the vendor may not handle and or store information within LHP appropriately according DOI's records policy. The vendor provides system operation and maintenance including monitoring of end-users and administrators, and appropriate Privacy Act clauses were inserted into the contract. LHP is categorized as a "Moderate" impact level system and is in the process of being certified by the Federal Risk and Authorization Management Program (FedRAMP). The privacy risks are mitigated throughout the information lifecycle. All user activities in LHP are monitored, and access is granted based on "need-to-know" to perform their official duties on behalf of DOI. All application and operator actions are logged and stored in an isolated system with a very Limited Access policy, and all user access attempts to the system are timestamped. DOI SOL is responsible for assigning access based on least privileges and the appropriate use of data in LHP. Also, SOL personnel with access to LHP take part in DOI annual IT security and Privacy training.

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 Office of the Solicitor has an ethical obligation to advise the Department that it must take reasonable steps to preserve information that is relevant to the claims and defenses of active or reasonably anticipated litigation. The data being collected allows the Office to meet its professional responsibility and allows the Department to take the reasonable steps that are necessary to preserve the potentially relevant information.

☐ 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

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: Office of the Solicitor
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other:

The SOL system administrator assigns individual users into one of several user groups with different levels of access rights. When a particular SOL employee is handling a particular legal hold matter, that user will be allowed to see which custodians have been identified and associated with that matter.

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

Users are given access based on their role in the Solicitor's Office. For example, legal staff with responsibilities related to employment data would only be given access to the data applicable to employment case tracking, and legal staff with no responsibility to employment case tracking would not be able to access to that data.

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.

Contractors were involved with the design and configuration of the system and will be involved with the maintenance and operation of the system. Federal Acquisition Regulations (FAR) contract Clause 52.224-1, Privacy Act Notification (April 1984), FAR contract Clause 52.224-2, Privacy Act (April 1984), FAR contract Clause 52.239-1, Privacy or Security Safeguards (August 1996) and 5 U.S.C. 552a are included by reference in the agreement with the contractor.

☐ 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.

All user and administrator actions within LHP are logged and stored in an isolated system with a very Limited Access policy.

☐ No

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

All application and operator actions are logged and stored in an isolated system with a very Limited Access policy. Actions logged include: all user access attempts to the system; date and time of access; account provisioning/de-provisioning and privilege escalation events; modification of system/application security settings or sensitive information as defined by the information system to include specific criteria for transaction access and manipulation types (Create, Read, Update, Delete (CRUD)) and deemed to be a risk to the mission/business function of the information system; modifications, deletes, or purging of any audit records or audit log file settings either system generated or via application generation.

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

System audit logs are restricted, but can be accessed as needed for troubleshooting, performance monitoring, and incident response investigations.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption

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

(3) Administrative Controls. Indicate all that apply.

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

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 Legal Hold Pro Information System Owner within the Office of the Solicitor is the official responsible for oversight and management of the Legal Hold Pro security and privacy controls, including the protection of the information processed and stored by the system. The Legal Hold Pro Information System Owner and the Information System Security Officer are responsible 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 in Legal Hold Pro system in consultation with Departmental Offices Associate Privacy Officer.

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 Legal Hold Pro Information System Owner is responsible for the daily operational oversight and management of the Legal Hold Pro security and privacy controls, 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. The Legal Hold Pro

Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, or unauthorized access or disclosure of the PII is reported to DOI-CIRC and appropriate DOI officials in accordance with Federal policy and established DOI procedures.