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: Office of the Solicitor Information System (SOLIS)
Bureau/Office: Office of the Solicitor
Date: April 21, 2020
Point of Contact:
Name: Danna Mingo
Title: Associate Privacy Officer, Office of the Secretary
Email: OS_privacy@ios.doi.gov
Phone: 202-208-3368
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 Office of the Solicitor Information System (SOLIS) is designed to enable SOL staff, attorneys, and leadership to manage and track its work, including both litigated and non-litigated matters. SOLIS will replace the decentralized tracking systems that currently exist throughout SOL with a single collaboration, information-sharing, and resource-allocation tool.

The purpose of the system is to assist attorneys in the Office of the Solicitor in providing legal services to the Department of the Interior (DOI) personnel on a wide variety of legal issues; provide legal advice to DOI officials; maintain necessary information on individuals who are, or will be, in litigation with the Department, as well as their attorneys or representatives, to represent DOI during litigation and related activities; respond to claims by employees, former employees, and other individuals; assist in the settlement of claims against the government; and manage case files related to litigation and appeals.

C. What is the legal authority?

43 U.S.C. 1455; 5 U.S.C. 301, 551 et seq.; 16 U.S.C. 791 et seq.; 25 U.S.C. 2, 9, 372, 373, 373a, 373b, 374, 2201 et seq.; 30 U.S.C. chap. 2, 3, 3A, 5, 7, 16, 23, 25 and 29; 41 U.S.C. 7101 et seq.; 43 U.S.C. 315a, 1201, 1331 et seq., 1601 et seq., 1701 et seq.; 43 CFR parts 4, 30, and 45.

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: The Office of the Solicitor wants to consolidate the various tracking systems (i.e. spreadsheets, Word docs, etc.) into one system.

E. Is this information system registered in CSAM?

☒ Yes: Office of the Solicitor Information System CSAM ID 2561
☐ 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: The records in the SOLIS system are covered under the various Office of the Solicitor's SORNs found at the following link: https://www.doi.gov/privacy/sol-notices. The SORNs are currently being modified and updated.
☐ 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	☐ Religious Preference	☐ Social Security Number (SSN)
☐ Citizenship	☐ Security Clearance	☒ Personal Cell Telephone Number
☐ Gender	☐ Spouse Information	☐ Tribal or Other ID Number
☐ Birth Date	☐ Financial Information	☒ Personal Email Address
☐ Group Affiliation	☐ Medical Information	☐ Mother's Maiden Name
☐ Marital Status	☐ Disability Information	☒ Home Telephone Number
☐ Biometrics	☐ Credit Card Number	☐ Child or Dependent Information
☒ Other Names Used	☐ Law Enforcement	☐ Employment Information
☐ Truncated SSN	☐ Education Information	☐ Military Status/Service
☐ Legal Status	☐ Emergency Contact	☒ Mailing/Home Address
☐ Place of Birth	☐ Driver's License	☐ Race/Ethnicity

☒ Other: Attachments may be uploaded to the system and may contain PII associated with the litigation being tracked. These attachments will include briefing materials and/or public records downloaded from the PACER (Public Access to Court Electronic Records) system. These attachments will not contain sensitive PII that has not been identified above.

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: Download from PACER (Public Access to Court Electronic Records)

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

The system will use PII to identify the individuals who are involved in the litigated or non-litigated matters being tracked and managed in the system. SOL users may also possibly use these individuals' personal email or physical addresses when, in the normal course of their business with the Department, they have asked to be contacted via their personal email address or physical address.

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

☒ Within the Bureau/Office: SOL users may rely on the PII entered by other SOL users in order to send communications related to the matters that they are handling.

☒ Other Bureaus/Offices: Other bureaus and offices will be provided data from the system to enable them to track the litigation in which they or their employees or contractors are involved.

☒ Other Federal Agencies: Data may be shared with the Department of Justice as a record of the Department's litigation efforts, and with other Federal agencies as authorized under other routine uses outlined in the SOL-I, 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: Contractors who are involved with the design, configuration, maintenance and operation of the system will have access to the PII.

☐ 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.*

☒ No: The Department must be able to identify and communicate with individuals who are involved in litigated and non-litigated matters affecting the Department.

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

☒ Privacy Act Statement: When information is collected directly from an individual covered under the appropriate system of records notice and Privacy Act Statement prior to the collection of data.

☒ Privacy Notice: Privacy notice is provided through the publication of this privacy impact assessment and the appropriate Office of the Solicitor's system of records notice published in the Federal Register and found at the following link: https://www.doi.gov/privacy/sol-notices.

☒ Other: The system is configured to provide a Rules of Behavior that is acknowledged by the users of the system. The Rules of Behavior outlines the responsibility to protect the PII within the system and the user's responsibility to protect the privacy of the individuals. Role-based training is also provided to the users of the system.

☐ None

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. SOL employees and contractors will also be able to retrieve records by the names or email addresses of individuals who are involved in the litigated or non-litigated matters being tracked and managed in the system.

I. Will reports be produced on individuals?

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

☒ No

Section 3. Attributes of System Data

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

Not Applicable. Data is collected from DOI records.

B. How will data be checked for completeness?

The PII stored by the system will be obtained from 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 PII of individuals involved in litigated or non-litigated matters affecting the Department will be updated as they are identified and added to the system. These individuals' names and email addresses will also be updated upon the discovery of any failure of communications between the Office of the Solicitor and the individuals.

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

SOLIS records pertaining to litigated and non-litigated matters are maintained under Departmental Records Schedule (DRS) 3.2.0006, Document Collection and Legislative Input Records which is approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0008-0006). Such records include documents created and maintained for response to judicial or legislative issues; interpretation/explanation of litigation records certifying response to a collection, copies of records assembled for response to a collection (but not the original records, which must be returned to the office of origin), and other records developed in administering response to a collection. Records should be cut-off (made inactive/archived) when no longer relevant to litigation, then destroyed 8 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?

SOLIS records will be maintained for the life of the records, as DOI deems necessary to meet litigation and appeal defense needs, then destroyed after cutoff in accordance with the DRS 3.2.0006, Document Collection and Legislative Input Records schedule, by approved methods under 384 Department Manual 1 and 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 minimal risk to SOL employee and contractor privacy as the user information consists of name and official email address that are not considered sensitive PII. The individuals who are involved in litigated and non-litigated matters affecting the Department do have a discernible privacy interest in their names and email addresses, but the Department must be able to identify and communicate with those individuals.

There is a small 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 the Office's requirements to track litigated and non-litigated matters and meet the legal needs and obligations of the Department. There is a risk of maintaining inaccurate information that may result in misdirected communications. This risk is mitigated through established procedures to verify correct information for individuals who are involved in litigated and non-litigated matters affecting the Department.

There is a minimal risk that unauthorized individuals may access the information in SOLIS or use it for an unauthorized purpose. This risk is mitigated by ensuring effective access controls are implemented, only granting authorized personnel access to SOLIS, and requiring system users to agree to adhere to the DOI Rules of Behavior. There is also a risk that information in SOLIS 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.

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 SOLIS appropriately according to DOI's records policy. Salesforce.com, Inc., provides system operation and maintenance including monitoring of end-users and administrators, and appropriate Privacy Act clauses were inserted into the contract. SOLIS is categorized as a "Moderate" impact level system, and the Salesforce platform upon which it was built has been certified by the Federal Risk and Authorization Management Program (FedRAMP). The privacy risks are mitigated throughout the information lifecycle. All user activities in SOLIS are monitored, and access is granted to users based on their "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 the lowest level of privileges necessary. Also, SOL personnel and contractors with access to SOLIS 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 performs the legal work of the Department and has an obligation to perform that work efficiently and competently. The data being collected allows the members of the Office to meet their professional responsibility obligations and allows the Department to reasonably manage its legal obligations.

☐ 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.

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*

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

The system will utilize an access control list that will give users access based on their role in the Office of the Solicitor.

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?*

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. *Explanation*

☒ No

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

☒ Yes. All user and administrator actions within SOLIS are logged and stored.

☐ 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. Actions logged include: all user attempts to access the system, including the date and time of each access attempt; 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; modification, deletion, or purging of any audit records or audit log file settings, whether system-generated or generated via the application.

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

System audit logs are restricted to SOL personnel and contractors only 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 SOLIS Information System Owner within the Office of the Solicitor is the official responsible for oversight and management of the SOLIS security and privacy controls, including the protection of the information processed and stored by the system. The SOLIS 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 SOLIS in consultation with DOI Privacy Officials.

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 SOLIS Information System Owner is responsible for the daily operational oversight and management of SOLIS 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 SOLIS 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.