



# PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. *All entries must be Times New Roman, 12pt, and start on the next line.* If you need further assistance, contact your LPO. A listing of the LPOs can be found here:

[https://usepa.sharepoint.com/:w:/r/sites/oei\\_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name:</b> Enterprise Legal Case Management System (ELCMS)	<b>System Owner:</b> Michael Hardy
<b>Preparer:</b> Nicole Williams	<b>Office:</b> Strategic IT Investment Staff, OMS
<b>Date:</b> 10/14/2021	<b>Phone:</b> 202-564-4026
<b>Reason for Submittal:</b> New PIA <input type="checkbox"/> Revised PIA <input checked="" type="checkbox"/> Annual Review <input type="checkbox"/> Rescindment <input type="checkbox"/>	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/> Development/Acquisition <input checked="" type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
<b>Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></b>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u><a href="#">OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</a></u></b>	

## **Provide a general description/overview and purpose of the system:**

The OALJ E-Filing System Privacy Impact Assessment and EPA-66 previously published system of record notice for Case Records System will transfer to the modified system of record notice for Enterprise Legal Case Management System to manage information contained in the system is primarily for the purpose of Agency Judges, Attorneys and Clerks to render determinations with respect to matters before them and communicating the determinations to the appropriate individuals and organizations, as well as to the general public. When fully implemented, the electronic filing portion of the system will provide for online filing, tracking, and accounting of filings (e.g., pleadings, motions, briefs, exhibits, orders, and determinations) in all cases, both pending and archived. Other uses of the system and the information contained, therein, include:

- Responding to Freedom of Information Act requests;

- Providing management information necessary to assess workload, assign incoming cases and monitor case progress;
- Allowing individual judges to monitor the progress of assigned cases;
- Providing ready access to case docketing information to support staff to enable timely response to complainants, government and private counsel, and respondents concerning the status of a particular case; and
- Promoting adjudicative transparency by providing public access to Agency litigation documents.

## **Section 1.0 Authorities and Other Requirements**

### **1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?**

42 U.S.C. 11001 et seq. (Emergency Planning & Community Right-to-Know Act (EPCRA)); 42 U.S.C. 6901 et seq. (Resource Conservation and Recovery Act (RCRA)); 15 U.S.C. 2601 et seq. (Toxic Substances Control Act (TSCA)); 7 U.S.C. 136 et seq. (Federal Insecticide, Fungicide and Rodenticide Act (FIFRA)); 42 U.S.C. 9601 et seq. (Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)); 33 U.S.C. 1251 (Federal Water Pollution Control Act (FWPCA), commonly known as the Clean Water Act (CWA)); 42 U.S.C. 7401 (Clean Air Act (CAA)); 40 CFR 22.4 (Consolidated Rules of Practice Governing the Administrative Assessment of Civil Penalties and the Revocation/Termination or Suspension of Permits).

### **1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?**

The Agency's Business Automation Platform (BAP) Salesforce has an EPA Authority to Operate at the FISMA Moderate level. It expires July 19, 2024.

### **1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

No ICR Required

### **1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?**

The EPA's Business Automation Platform (BAP), powered by the Salesforce Force.com Platform as a Service (PaaS), is a shared multi-tenant environment hosted in the Salesforce GovCloud.

The BAP is built specifically on the Salesforce Government Cloud, which is a cloud-hosted, PaaS environment that meets the unique security needs of the Federal Government, including FedRAMP, NIST, and DISA IL2 (IL4 pending)

## **Section 2.0 Characterization of the Information**

*The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.*

### **2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).**

Parties may submit a wide range of document types to the Agency containing various types of information including, but not limited to, names, addresses, social security numbers, medical and/or financial information contained in opinions of law, pleadings, motions, exhibits, and other documents submitted by the parties to a matter and the presiding Judges. This includes information found in individual tax returns and other documents related to a party's ability to pay a monetary civil penalty.

### **2.2 What are the sources of the information and how is the information collected for the system?**

The sources of information in the system are limited to documents submitted by the parties to a matter (e.g., briefs, motions, exhibits) and by the judges presiding over the matter (e.g., orders, initial decisions). Parties may submit a wide range of document types to the Agency containing various types of information.

### **2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

No information is from commercial sources.

### **2.4 Discuss how accuracy of the data is ensured.**

The accuracy of the data is maintained by the entities the data is sourced from. As data is updated in ELCM, the Users of the system are responsible for validating the information and actions associated with their cases in ELCM.

### **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

*Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.*

#### **Privacy Risk:**

There is a low risk of having the information collected disclosed to unauthorized users if the security controls implemented within the BAP were ever breached.

## **Mitigation:**

Currently, only those with valid EPA LAN credentials have access to the BAP. As part of the Enterprise Single Sign-On (ESSO) initiative, EPA users can now use their PIV cards to login to the BAP without needing to enter their User ID and Password. There are also access control levels that limit users' view/edit access to legal cases that are either their own or assigned to them for review/approval.

## **Section 3.0 Access and Data Retention by the System**

*The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.*

### **3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?**

The Platform uses all the extensive access controls of the Salesforce force.com service, including user and group profiles, permission sets, object-level permissions, record-level permissions, field-level permissions, and other fine-grained access controls. The BAP enforces access control levels on data and functions available to any user according to the user's role, based on need to know. Access control levels include Administrator, Delegated Administrator, and application-specific levels. Each application in the BAP has a unique security profile restricting access to its data to those with a need to access it. The BAP enforces access restrictions by roles for each application, granting access to specific functionality and particular data as required by the application's design approved by the application owner.

### **3.2 In what policy/procedure are the access controls identified in 3.1, documented?**

Detailed information is available in the salesforce security implementation guide. [http://login.salesforce.com/help/pdfs/en/salesforce\\_security\\_impl\\_guide.pdf](http://login.salesforce.com/help/pdfs/en/salesforce_security_impl_guide.pdf).

### **3.3 Are there other components with assigned roles and responsibilities within the system?**

No there no other components.

### **3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?**

Most of the information contained in the ELCM System will be accessible to EPA staff. This may include not only case parties and Judges but those individuals with a valid EPA email address. The public will not have access to documents containing data protected by the Privacy Act unless an exemption or exception applies.

The ELCM Development Team does consist of contractors. The contract did include the appropriate FAR clauses.

**3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.**

Yes, EPA Records Schedules 508, 509, and 510 apply to the Enterprise Legal Case Management System. Records are retained as long as needed to conduct Agency business and historical legal research. After 15 years of closure, they are transferred to the National Archive.

**3.6 Privacy Impact Analysis: Related to Retention**

*Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.*

**Privacy Risk:**

There's a possible risk or retaining records longer than needed.

**Mitigation:**

To mitigate the risk, periodic review and implementation of the record control schedule are performed.

## **Section 4.0 Information Sharing**

*The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.*

**4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.**

No. There is no external sharing.

**4.2 Describe how the external sharing is compatible with the original purposes of the collection.**

N/A

**4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?**

N/A

#### **4.4 Does the agreement place limitations on re-dissemination?**

N/A

#### **4.5 Privacy Impact Analysis: Related to Information Sharing**

*Discuss the privacy risks associated with the sharing of information outside of the agency.  
How were those risks mitigated?*

##### **Privacy Risk:**

There is no risk.

##### **Mitigation:**

There is no mitigation.

### **Section 5.0 Auditing and Accountability**

*The following questions are intended to describe technical and policy-based safeguards and security measures.*

#### **5.1 How does the system ensure that the information is used as stated in Section 6.1?**

Through the levels of approval required to complete a legal case as well as through periodic audits performed by the ELCM Team.

#### **5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.**

EPA Employees must take the Agency's Information Security and Privacy Awareness Training annually.

#### **5.3 Privacy Impact Analysis: Related to Auditing and Accountability**

##### **Privacy Risk:**

There is a low risk of unaccounted for changes/data due to the current limitation the system must track changes.

##### **Mitigation:**

We do ensure changes can only be made by the person it is currently assigned to or a BAP Admin. Those with BAP Admin access have been instructed by the Application owner and BAP COR to never approve on behalf of someone. This has been communicated verbally and via email. They predominately assist in reassigning requests when the person assigned is out of office; the email requesting the change is captured in the approval history when doing so. They encourage users to make changes themselves and try to limit their actions to instructing users.

## Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

### 6.1 Describe how and why the system uses the information.

As stated above in general description, the information contained in the ELCM System is primarily for the purpose of enabling Judges to render determinations with respect to matters before them and communicating those determinations to the appropriate individuals and organizations, as well as the general public.

### 6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes X No   . If yes, what identifier(s) will be used. (A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

Cases are retrieved by the business entity, names of the parties to a particular case, or the docket number.

### 6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The consideration of Privacy Controls is inherently built in or addressed at the platform. The BAP enforces access control levels on data and functions available to any user according to the user's role, based on need to know. Access control levels include Administrator, Delegated Administrator, and application-specific levels. Each application in the BAP has a unique security profile restricting access to its data to those with a need to access it.

Security controls used to protect personal sensitive data in Enterprise Legal Case Management System are commensurate with those required for an information system rated MODERATE for confidentiality, integrity, and availability, as prescribed in National Institute of Standards and Technology (NIST) Special Publication, 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5.

1. *Administrative Safeguards:* EPA personnel are required to complete annual agency Information Security and Privacy training. EPA personnel are instructed to lock their computers when they leave their desks.
2. *Technical Safeguards:* Electronic records are maintained in a secure, password protected electronic system. ELCM access is limited to authorized, authenticated users integrated with the Agency's single-sign-on. This integration uses the user's LAN credentials to identify the user prior to granting access to the platform and ELCM system. All the system's electronic communication utilizes the agency's Trusted Internet Connection (TIC) for all transactions.

3. *Physical Safeguards:* All records are maintained in secure, access-controlled areas or buildings. Paper records are maintained in locked file cabinets. EPA personnel are required to complete annual agency Information Security and Privacy training. EPA personnel are instructed to lock their computers when they leave their desks.”

## **6.4 Privacy Impact Analysis: Related to the Uses of Information**

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

### **Privacy Risk:**

There’s a possible risk of data misuse by a user in ELCMS.

### **Mitigation:**

Mitigation to the privacy risk for Use is described in the BAP Security Plan with controls that requires login using Agency LAN ID and password in accordance with FISMA Moderate level controls specified in the BAP security plan. Accounts and audit logs are reviewed regularly.

**\*If no SORN is required, STOP HERE.**

*The NPP will determine if a SORN is required. If so, additional sections will be required.*

## **Section 7.0 Notice**

*The following questions seek information about the system’s notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.*

### **7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, [privacy@epa.gov](mailto:privacy@epa.gov).

### **7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?**

Yes. Parties need not submit any information they do not wish to provide. Failure to provide information relevant to a party's case, however, may diminish that party's likelihood of prevailing in the case. With respect to PII, the Agency encourages parties to either redact PII in documents being submitted to the Enterprise Legal Case Management System or refrain from submitting such documents altogether. If a party believes certain PII in a document is relevant to a determination being sought, the party may submit an electronic, redacted version of the document to the Enterprise



Legal Case Management System and a physical, un-redacted version to the Hearing Clerk.

### **7.3 Privacy Impact Analysis: Related to Notice**

*Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.*

#### **Privacy Risk:**

There's a possible privacy risk of Notice that users miss reading during log in.

#### **Mitigation:**

A mitigation to the possible risk of Notice is that Users are required to select a checkbox during the login that they have read and agree with the notice regarding privacy and confidential business information.

## **Section 8.0 Redress**

*The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.*

### **8.1 What are the procedures that allow individuals to access their information?**

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

### **8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

### **8.3 Privacy Impact Analysis: Related to Redress**

*Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.*

#### **Privacy Risk:**

There's a possible privacy risk of Redress if users aren't aware how to correct their information within ELCM. There is an appropriate process for Redress.

#### **Mitigation:**

There is an appropriate process for Redress identified in the ELCM System of Record Notice.