

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

System Name: ORD Assists Tracker		
Preparer: Kelly Dipolt	Office: ORD/CESER/TSCD	
Date: 1/14/2021	Phone: 513-569-7333	
Reason for Submittal: New PIA <input checked="" type="checkbox"/> Revised PIA <input type="checkbox"/> Annual Review <input type="checkbox"/> Rescindment <input type="checkbox"/>		
This system is in the following life cycle stage(s):		
Definition <input type="checkbox"/>	Development/Acquisition <input checked="" type="checkbox"/>	Implementation <input type="checkbox"/>
Operation & Maintenance <input type="checkbox"/>	Rescindment/Decommissioned <input type="checkbox"/>	
<p>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>.</p> <p>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45)</u>.</p>		

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

The system manages all of ORD's technical support, from the initial request and triage to support given, with analysis and reporting available throughout the process. This system will reside in the EPA BAP Platform.

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?

The following legal authorities direct EPA to provide technical assistance to States, municipalities and others. Assistance cannot be offered without knowing to whom to send the technical support.

From Safe Drinking Water Act (SDWA) Section 1442(2)(A):

The Administrator shall, to the maximum extent feasible, provide technical assistance to the States and municipalities in the establishment and administration of public water system supervision programs (as defined in section 1442(c)(1)).

<https://www.govinfo.gov/content/pkg/CPRT-106SPRT67528/pdf/CPRT-106SPRT67528.pdf>

From Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) Section 104(k)(7):

The Administration may provide, or fund eligible entities or nonprofit organizations to provide training, research, and technical assistance to individuals and organizations, as appropriate, to facilitate the inventory of brownfield sites, site assessments, remediation of brownfield sites, community involvement, or site preparation.

From Resource Conservation and Recovery Act (RCRA) Section 6913: The Administrator shall provide teams of personnel, including Federal, State, and local employees or contractors (herein referred to as “Resource Conservation and Recovery Panels”) to provide Federal agencies, States and local governments upon request with technical assistance on solid waste management, resource recovery, and resource conservation. Such teams shall include technical, marketing, financial, and institutional specialist, and the services of such teams shall be provided without charge to State or local governments.

<https://uscode.house.gov/view.xhtml?path=/prelim@title42/chapter82&edition=prelim>

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?

Salesforce platform authorized by OSM/OEI for agency use. Not accessible without an EPA email address. Salesforce has its own security plan which our system falls under and that is September 30, 2021.

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?

Yes, the data will be stored in the Salesforce EPA cloud. The Salesforce cloud has an ATO expiring on September 30, 2021. The Lighting Platform is PaaS.

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).

External people each provide their name, professional affiliation, phone and/or email, city, and state when requesting ORD assistance.

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

External people give the info described in 2.1 to an EPA employee, who enters it into this system.

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.

2.4 Discuss how accuracy of the data is ensured.

Data provided is entered manually exactly as provided. No verification needed.

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:

Low risk. The ORD staff might misinterpret the request while doing data input.

Mitigation:

There is a review process in place for staff to correct the mistake/mistakes when inputting the data.

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?

There will be roles assigned within BAP which will determine access-levels. The BAP uses all the extensive access controls of the Salesforce Lightning Platform, including user and group profiles, permission sets, object-level permissions, record-level permissions, field-level permissions, and other fine-grained access controls. Detailed information is available at http://login.salesforce.com/help/pdfs/en/salesforce_security_impl_guide.pdf.

ORD Employees: Create and edit their own entries

ORD Supervisors: View, review, and edit their group's entries

Triage Team: View, review, and edit any entry in the system

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

The Salesforce admins provide different level of access based on guidance from the ORD Assists Coordinators. Access is determined through assignment of Salesforce Lightning Platform permission sets. The procedure for requesting access to an application through its permission set(s) is documented in the BAP User Provisioning Guide in the BAP Community Site.

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

No.

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?

The system is developed & maintained by contractors who do have the FAR clause in their contract. No other contractors have (or will have) access to this system. Required EPA staff will also have access to the system EPA staff

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.

EPA 0088 – Bibliographic and Reference Systems – is the records schedule to use for the automated system. This retention covers the data input into the tool. When the system is used to generate a report using the information in it, it will fall under EAP 1006 – Administrative Management. The retention for EPA 0088 is 2 years after completion of

action and when no longer needed, and the retention for EPA 1006 is 6 years.

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:

If the data is retained longer than needed.

Mitigation:

No data will be retained more than what is noted in the EPA Records schedule.

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. Information is not shared externally.

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

N/A (see answer to 4.1).

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:

No risk since the information is not shared with external parties.

Mitigation:

N/A

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 in accordance with stated practices in this PIA (Section 6.1)?

The data is used for only the purpose it is collected. There are track changes within BAP system which lets us know who all access the data and tracks all changes to this record. Generally, only immediate management of each ORD Center or Offices have access to the data.

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

None other than the annually required Information Security and Privacy Awareness Training. First time users are also trained on ORD Assists Tracker system.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

The risk exists that applications being hosted on the BAP could have inadequate privacy controls at the application level, not taking sufficient advantage of the controls provided by the platform. Auditing may expose risks. Application owners are accountable to mitigate risks.

Mitigation:

OMS will manage all risks associated with Auditing and accountability. In conducting Conceptual Review, Design Review, and Production Readiness Review for an application, the BAP Platform reinforces that the application must have sufficient privacy auditing and accountability controls in place.

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.

The requestor contacts ORD, then an ORD employee inputs the request into the system. The request is then reviewed by the triage team. The system tracks the status of the process.

- 6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X_. 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.)

It is retrieved by a request ID (computer generated number) or by topic-area or by Center. We do **NOT** intend to retrieve requests by any person's name.

The data will be retrieved by the automatically generated number generated by Salesforce

- 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?**

There are controls in place to protect PII in the system.

Lab Contacts - have privileges to enter the request submitted to them.

ORD Assists triage team has elevated privileges to access system, and approve workflow.

ORD Center managers have Read rights to all data put in by their centers

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 is a low risk associated to data misuse

Mitigation:

The database has user timestamp feature that indicates who modified the system and at what time it was modified. Privacy risk mitigation is a function of both the source systems and the BAP security plan, which describes in detail the controls in place for the BAP. For example, the Business Automation Platform requires login using Agency LAN ID and password in accordance with FISMA Moderate level controls specified in the BAP security plan.

***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.

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?

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:

Mitigation:

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?

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

8.3 How does the system notify individuals about the procedures for correcting their information?

8.4 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:

Mitigation: