EPA United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Qualtrics	
Preparer: Velez Childress	**Office: ORD/OSIM**
Date: 10/01/2019	**Phone: 919-541-4583**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition □ Development/Acquisition ☒ Implementation □	
Operation & Maintenance □ Rescindment/Decommissioned □ **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 OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

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

Office of Research and Development (ORD) needs an online survey tool that can handle simple questionnaires to very complex survey's with extensive analysis. The ORD uses the Qualtrics Research Suite as its standard survey builder software. The software is owned and externally hosted by Qualtrics and provides ORD with the ability to generate and manage web-based surveys. It also offers a variety of reporting and analytics tools that allow authorized ORD users to track survey results and easily configure custom reports to meet survey requirements.

Surveys are administered on an external server and sent to survey participants via hyperlink, either by email or by posting the link online to ORD.gov. All requests to administer surveys must be approved by the appropriate ORD Office or Center and align with ORD's internal policy for collecting and protecting Personally Identifiable Information (PII). Surveys are typically used by ORD to collect data from survey respondents, which may include a limited amount of PII (i.e., their names and personal contact information), non-sensitive business information, and work-related contact information (i.e., work email address, work, telephone number, etc.). For example, PII may be collected in a survey on individuals interested in registering for ORD events/conferences, contact information may be requested to follow-up on survey questions but this request is optional and may or may not be provided by individuals being surveyed. In instances where ORD is conducting research, ORD may use Qualtrics surveys to notify collaborators about new environmental tools or models. In these instances, a Qualtrics survey may need to collect the names, email addresses, and telephone numbers of customers who want to give feedback on the tool or models usability, this request is optional and may or may not be provided by individuals being surveyed. The email addresses and telephone numbers collected from customers may be personal or work-related, depending on what the customers choose to provide. No sensitive PII will be collected by this application. All survey's are a part of the purpose that has been identified in this PIA.

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?

Reference Type:
Statute 44 USC §3501 et seq. (1980)
Paperwork Reduction Act (PRA)

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 SSP is under development and is recorded in XACTA. ORD is in the process of obtaining an ATO from the EPA. Qualtrics has a P-ATO from FedRamp and an SSP on file with FedRamp.

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.

Multiple survey forms will be required as external surveys are developed. ORD is in the process of obtaining an OMB Control number for Evaluating Customer Satisfaction of EPA's Research Products (ICR No. 2593.01) and will be filing for a Generic Clearance of Customer Satisfaction Surveys.

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?

Qualtrics is FedRamp approved as a SaaS, at moderate impact level, has a Government Community Cloud deployment model.

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).

The survey tool will collect information on various administrative and research topics. Data elements may contain PII (e.g. names, email addresses, work email address, and work telephone number of survey recipients).

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

The source of the information is individual respondents and data is collected via the cloud. Information in Qualtrics may be entered manually by authorized users. For surveys that are distributed via email or require authentication, the authorized ORD Office or Center survey Coordinator uploads or builds an invitation list in the survey software, which may contain PII (e.g. names and email addresses of survey recipients). Information may also be directly collected from individual respondents participating in the survey. Links to surveys can be published to both ORD.gov and may also be distributed by email to survey respondents. Limited PII may be collected (such as names) as well as non-sensitive data and work-related contact information (e.g., work email address, work telephone number).

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

Yes, the system collects survey data from individual respondents both internal and external to the Agency. The survey data is collected to evaluate end user satisfaction with EPA's Research Products and/or evaluate employee satisfaction with work related environment/services/programs.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the survey is ensured based on use of standard statistical measures and how much the responses deviates from the anticipated responses for each question/survey (i.e.

outliers).

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:

The data collect by the survey is unique to each survey. The risk associated with data collected in an individual survey is that PII such as name, email address, and phone numbers collected for individual respondents could potentially be disclosure to unauthorized individuals.

Mitigation:

Only authorized ORD Office and Center Survey Coordinators have access to the Qualtrics website to develop and implement surveys for their respective Office/Center. After deploying a survey, the Office/Center Survey Coordinators then have access to the survey data and download a local copy of the data for use with Microsoft Excel, Word, or PowerPoint to conduct further analysis and reporting. Authorized Office/Center Survey Coordinators may export survey data containing PII for tabulation and reporting purposes. Exported data and survey results are provided to authorized ORD employees and managers (i.e., survey customers/requestors) in the ORD Office/Center on a "need-to-know" basis in support of authorized business needs. Survey Coordinators are responsible for complying with all policies and procedures governing the use and maintenance of PII in a survey as outlined in the Rules of Behavior signed by the coordinator and the annual privacy training required of all EPA employees.

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?

Yes, authorized controls have been put in place. Only one Office/Center Survey Coordinator is assigned to each project. The survey coordinator can only assess the survey data held in the Qualtrics cloud using an assigned assess link provided by the Survey Administrator. After gaining access to the software, each survey coordinator must register a password to create and access the survey data.

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 survey tool requires a license and the policy for requiring a license is a signed contract with Qualtrics for use of the system and access control is documented in the policy to the application.

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 administrator, survey coordinator are the only persons that will have access to the data. Survey participants will have access to the system to complete the survey. All administrative roles mentioned above are federal employees, no contractors will be administering this system.

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.

The survey data is not retained in the system after the analysis is completed. The survey analysis time period will not exceed 30 days after completion of a survey. Survey reports can be downloaded from the system to share survey outcomes. General questionnaires/surveys are considered Program Mgmt files and are retained under EPA Records Schedule 1006b, and questionnaires that collect data for research would be held under the research schedule EPA Records Schedule 1035.

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:

Privacy data is retained in the Qualtrics GovCloud and can be downloaded to the EPA and stored on EPA secure servers. The risk relating to retention is that the survey coordinator might misuse the data for an authorized purpose or that the data might be retained for unauthorized period.

Mitigation:

No third-party organization will have access to PII. All response data is retained in Amazon Web Services (AWS) GovCloud (environment is specific only for Federal customers), and data is protected by disk level encryption and database encryption. AWS GovCloud has an existing ATO (Authority to Operate) under FedRAMP, which gives Government agencies the ability to leverage AWS GovCloud for sensitive workloads.

At the end of the retention period, surveys can be deleted. Since Qualtrics uses the data isolation service, a key hierarchy is created for each Federal customer. Key management is via Amazon Web Services Key Management Service (KMS). Each customer has a unique Key Encryption Key (KEK) used to encrypt and protect a series of unique Data Encryption Keys (DEK). A unique DEK is created for each customer survey. A federal customer may request key destruction of the customer specific KEK which leads to survey data destruction. The data decommissioning procedures are established by the federal customer.

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.

None of the interconnected systems have the ability to share, transmit or access PII in the Insight Platform. Survey data may be shared outside of EPA as a part of the survey and the survey coordinator will accept responsibility for securing the PII used in the analysis phase. The ROB will annotate this responsibility and it will be signed by the survey coordinator.

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

While results of a survey may be shared outside of the Agency, no PII generated from the survey will be shared outside of the Agency as documented in the ROB. There is no external sharing of PII.

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?

No information sharing agreements, MOUs or information sharing agreements are allowed by users of the Qualtrics survey tool. **There is no external sharing of PII**

4.4 Does the agreement place limitations on re-dissemination?

Sharing of PII generated by a survey is prohibited by the ROB. No. There is no external sharing of PII

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:

None. There is no external sharing of PII.

Mitigation:

None.

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 Qualtrics application is used for sole purpose for which the survey is requested and only in response to the requirements of each survey. Qualtrics can only be accessed with a link to the tool provided by the system administrator and which is given to the survey coordinator to conduct the required survey. The control that ensures that the survey tool and information gathered in the survey is used in accordance with the stated practice in this PIA is that no survey tool license is issued without a signed Rules of Behavior and compliance with the Paperwork Reduction Act if applicable. The oversight for this control is the issuance of the license by the ORD Qualtrics Coordinator.

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

Survey coordinators are required to take mandatory annual Information Security and Privacy Awareness training regarding the safeguarding of PII. Annual training covers the collection of any and all PII collected by the Agency.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Survey data that may contain PII is retained in the Qualtrics database on the secure Qualtrics Cloud. The risk is that during an audit all PII may not be accounted for and mitigated.

Mitigation:

The mitigation is that a 3rd party Continuous Monitoring Assessment (CMA) is in place to ensure that all PII controls are 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.

PII may be collected in a survey on individuals interested in registering for ORD events/conferences, contact information may be requested to follow-up on survey questions but this request is optional and may or may not be provided by individuals being surveyed. In instances where ORD is conducting research, ORD may use Qualtrics surveys to notify collaborators about new environmental tools or models. In these instances, a Qualtrics survey may need to collect the names, email addresses, and telephone numbers of customers who want to give feedback on the tool or models usability. The email addresses and telephone numbers collected from customers may be personal or work-related, depending on what the customers choose to provide.

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.)*

Survey data is retrieved by survey question which is assigned a unique identifier linked to the survey question.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

No

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 risk that the information may be used for a different purpose or unauthorized purpose.

Mitigation:

The survey tool requires a Rules of Behavior for how information is collected and the Continuous Monitoring Assessment (CMA) monitors that the ROB is signed annually.

*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: