

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: <u>https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx</u>

System Name: Qualtrics SaaS	
Preparer: Brian Stitt	Office: OMS OITO-ECSD
Date: 03/12/2024	Phone: 202-566-1638
Reason for Submittal: New PIA Revised PIA Annual Review_X 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	

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)</u> (pgs. 44-45).

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

OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

OMS is acquiring an online survey tool that can handle simple questionnaires to very complex surveys with extensive analysis. Formerly, FDIC uses the Qualtrics Research Suite as its standard survey builder software. The software is owned and externally hosted by Qualtrics and provides FDIC with the ability to generate and manage web-based surveys. It also offers a variety of reporting and analytics tools that allow authorized FDIC 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 a hyperlink, either by email

or by going to the following link online: https://epaenterprise.gov1.qualtrics.com/homepage/ui. All requests to administer surveys must be approved by the appropriate OMS Office or Center and align with OMS's internal policy for collecting and protecting sensitive information and Personally Identifiable Information (PII). Surveys are typically used by OMS to collect data from survey respondents, which may include a limited amount of PII (i.e., their names and personal contact information, work email address, work telephone number, etc.). For example, PII may be collected in a survey on individuals interested in registering for OMS events/conferences and contact information may be requested to allow for following up with the individual regarding the survey questions, this request is optional and may or may not be provided by individuals being surveyed. In instances where OMS is conducting research, OMS may use Qualtrics survey may need to collect the names, email addresses, and telephone numbers of customers who want to give feedback on the tool or model's 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.

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?

5 U.S.C. 301, Departmental Regulations; 44 U.S.C. Chapter 35, the Paperwork Reduction Act; 40 U.S.C. 1401, the Clinger-Cohen Act; 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; and Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.

- 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 has been recorded in XACTA and will continuously be reviewed annually for any changes/modifications if needed. System received its signed ATO on 7/31/2023 and will expire on 6/30/2026.
- **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.

OMS has obtained the OMB Control number 2080-0085 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?

The data is maintained and stored in the Government Community Cloud. Qualtrics is FedRAMP-approved as a SaaS, at a moderate impact level, and 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).

Qualtrics collects on various administrative and research topics in the form of surveys (some anonymous, others not). The survey may contain PII (e.g., names, personal email addresses, personal telephone numbers, 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 information is provided by the individual respondents and data is collected via the cloud. Information in Qualtrics SaaS may be entered manually by authorized users. For surveys that are distributed via email or require authentication, the authorized OMS Office or Center Survey Coordinator uploads or builds an invitation list in the survey software. Center Survey Coordinators analyze survey data and provide timely reports for senior staff by providing advice on survey sampling and statistical techniques to ensure survey methodology is statistically valid. It 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 be published can on https://epaenterprise.gov1.qualtrics.com/homepage/ui and may also be distributed by email to survey respondents.

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.

The accuracy of the survey is ensured by the center coordinators and once the survey is submitted the survey creator may edit/delete questions on the survey, but they cannot alter or delete responses.

2.5 <u>Privacy Impact Analysis</u>: 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 collected by the survey is unique to each survey. Privacy risk is associated with data collected in an individual survey that includes PII such as name, email address, and personal phone numbers collected from individual respondents. While PII elements processed by Qualtrics is not SPII, its sensitivity is raised by quantity (e.g., many surveys). Risks are associated with accuracy or credibility of sources because it is limited to the name and email addresses of the individual inputting the information.

Mitigation:

We deploy NIST 800-53 security and privacy controls to protect the PII processed by the system. Input validation of data sourced from respondents is in place to ensure accuracy and credibility of the data contained in survey information. All Qualtrics users must agree to the EPA Rules of Behavior, before accessing the system and or information stored in the system, which includes consent to monitoring, and restrictions on data usage.

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 access controls have been put in place. Controlled access is based on least privilege and need to know principles. 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 In what policy/procedure are the access controls identified in 3.1, documented?

Qualtrics has access control levels in line with EPA's access control policy which implements minimum functionality and principle of least privilege. The policy is accessible though EPA agency portal here: https://www.epa.gov/system/files/documents/2023-06/information_security_access_control_procedure.pdf.

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

The system implements two levels of roles to manage the Qualtrics platform and a role to manage group level administrative activities, the Brand Administrator and Division Administrator. The Brand Administrators are a group of individuals who are your point of contact for questions related to group level account set-up and management of Qualtrics users. The Division Administrator can handle division-related tasks. It's important to note that divisions are primarily used for managing permissions for a subset of users.

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 and 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. For all administrative roles mentioned above, they 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 thirty days after the completion of a survey. Survey reports can be downloaded from the Qualtrics GovCloud to share survey outcomes. General

questionnaires/surveys are considered Program Management files and are retained under EPA Records Schedule 1006b, and questionnaires that collect data for research will 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 retained in the Qualtrics GovCloud can be downloaded to the EPA and stored on EPA secure servers. The risk relating to retention is that survey data might be retained for an unauthorized period and that the Survey Coordinator might misuse the data for an unauthorized purpose.

Mitigation:

We conduct periodic reviews of the data to ensure that the data is not retained longer than authorized in the retention schedule. At the end of the retention period, surveys are deleted in line with the retention schedule. Also, Qualtrics uses data isolation service to keep it safe from internal threats. Access reviews are done to ensure accounts are valid.

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.

Survey data may be shared outside of EPA as a part of the survey to the survey participants, and the Survey Coordinator will accept responsibility for securing the PII used in the analysis phase. The Rules of Behavior will annotate this responsibility and it will be signed by the Survey Coordinator. There are no interconnections, sharing to non-survey participants, paper, print, or social media platforms.

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 Rules of Behavior.

Qualtrics does not share any information externally outside of the EPA. The purpose for the collection of the information is only through internal EPA individuals and retained within the Qualtrics system.

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?

There are no information sharing agreements, MOUs or information sharing agreements in relation to Qualtrics Survey tool. Information is not shared outside of EPA, except for survey results and those results are approved by signed Rules of Behavior (ROB). There are no other sharing agreements, MOUs, or other agreements in place at this time.

4.4 Does the agreement place limitations on re-dissemination?

Sharing of PII generated by a survey is prohibited by the Rules of Behavior. No controls needed to share survey analysis through Agency portal or by email with participants.

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:

Limited results from the survey are shared which could lead to some information on PII being leaked to unauthorized individuals inadvertently.

Mitigation:

All shared results are protected by Rules of Behavior and/or access control lists. The administrators and center coordinators are limited in nature to prevent any data leakage or information outside of EPA. Data Loss Protection has been implemented in Microsoft Outlook to detect PII in email.

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?

The Qualtrics application is used for the 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, 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 OMS Qualtrics coordinator.

In addition, NIST 800-53 auditing and accountability controls from the AR group are in place. These include assessment, continuous monitoring, configuration control, auditing (includes recommended logging practices) and OIG oversight.

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 all PII collected by the Agency.

5.3 <u>Privacy Impact Analysis</u>: Related to Auditing and Accountability

Privacy Risk:

Risk that unaccounted 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 possibly be provided to an unauthorized user. There is a risk that the system may not meet audit guidelines or be able to account for PII that was contained in surveys. If this information cannot be found this could lead to security incident or data leakage.

Mitigation:

The mitigation is that a third-party Continuous Monitoring Assessment (CMA) is in place to ensure that all PII controls are in place and allow auditing controls that allow administrators to protect this information. OIG oversight adds a layer to Agency accountability and auditing practices to secure sensitive data.

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 OMS 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 OMS is conducting research, OMS may use Qualtrics SaaS 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.)

The system is designed to retrieve information by the survey results. You cannot retrieve information by a personal identifier.

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?

System does not require a SORN. N/A.

6.4 <u>Privacy Impact Analysis</u>: 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 Rules of Behavior 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 <u>Privacy Impact Analysis</u>: 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 <u>Privacy Impact Analysis</u>: 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: