PRIVACY IMPACT ASSESSMENT

ECA Qualtrics Survey System

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: ECA Qualtrics Survey System
(b) System acronym: QUALTRICS
(c) Bureau: ECA
(d) iMatrix Asset ID Number: 292025
(e) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(f) Reason for performing PIA: New system
(g) Explanation of modification (if applicable): N/A

3. Purpose

(a) Describe the purpose of the system.

The mission of the Bureau of Educational and Cultural Affairs (ECA) is to increase mutual understanding between the people of the United States and the people of other countries by means of educational and cultural exchange that assist in the development of peaceful relations. At the heart of ECA's program design is survey data, collected from program participants and other stakeholders focused on perceptions of the programs and its impact on their lives. The data is part of a continuous learning cycle in which ECA and its implementing partners leverage data to determine what works best in programming and how programs can be improved going forward.

ECA's platform of choice for collection and analysis of survey data is Qualtrics, a FedRAMP cloud Software as a Service (SaaS) that helps drive the bureau's mission. Qualtrics offers powerful tools for design and dissemination of surveys, as well as analysis and visualization of survey data. In addition to this industry-leading functionality, Qualtrics is the only FedRAMP moderate authorized survey platform with approval for collection of personally identifiable information (PII) which provides ECA with greater options to collect the data necessary to further its objectives.

The Monitoring, Evaluation, Learning, and Innovation (MELI) unit at ECA routinely deploys these surveys but also trains and empowers the bureau's implementing partners to collect monitoring and evaluation data through Qualtrics. These coordinated efforts help ensure that data collection adheres to the highest-quality standards in a secure information environment. The end-result is data-driven decision-making that helps maximize ECA programs' efficacy and impact. The MELI team also employs Qualtrics

for internal purposes at ECA to gather information from staff on critical policy and performance matters.

(b) Personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The PII that the system collects are name, email address, phone number, country and state. This information is collected on both U.S. and non-U.S. persons; the remainder of the PIA will address the PII of U.S. persons only.

(c) How is the PII above collected?

The PII is collected directly from the record subject in response to a survey.

(d) What is/are the intended use(s) for the PII?

The intended uses for the PII depends on the individual survey and the team behind it. A typical scenario would be a survey asking participants whether they have experienced any problems in their program, and whether they would like someone from ECA to follow up about any problems reported. When the MELI (Monitoring Evaluation Learning and Innovation) unit collects PII in this way, it is always highlighted in the survey's consent script that: 1) entry of PII is optional; and 2) personal follow-up from ECA may occur if a survey participant enters their PII.

(e) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes

4. Authorities and Records

(a) What are the specific legal authorities and/or agreements that allow the information to be collected?

5 U.S.C. 301 (Management of the Department of State)
22 U.S.C. 1431 et seq. (United States Information and Educational Exchange Act of 1948, as amended; Smith-Mundt Act)
22 U.S.C. 2451-58 (Mutual Educational and Cultural Exchange Act of 1961, as amended; Fulbright-Hays Act)
22 U.S.C. 2651a (Organization of the Department of State)

(b) If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security number.
N/A

(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)? If yes, please indicate relevant System of Records Notice (SORN) below

☒Yes, provide:
- SORN Name and Number:
  STATE-08 Educational and Cultural Exchange Program Records 07/30/2020

☐No, explain how the information is retrieved without a personal identifier.

(d) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(e) List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system?

Disposition Authority Number(s):
- Program Support Records, DAA-0059-2019-0007-0010

5. Data Sources, Quality, and Integrity

(a) What categories of individuals originally provide the PII in the system?

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) Do the individuals listed in 5(a) provide PII on individuals other than themselves?

☐Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)
☒N/A

(c) What process is used to determine if the PII is accurate?

There is no official way to check the accuracy of the PII collected. The PII is collected directly from an individual (survey participant) and if incorrect PII is provided, the Program team will not be able to reach out to the survey participant for follow up purposes. ECA relies on the accuracy of the PII provided by the individual. ECA does not check the

information against any other source.

(d) What steps or procedures are taken to ensure the PII remains current?

ECA assumes that PII entered into a survey is current at the time of entry. There is no way to check the accuracy of the PII collected. The survey participant is responsible for keeping the information current. In cases where that PII is determined to be out-of-date, the data will be archived. The program teams use the PII to contact survey participants only for immediate follow up on the surveys content and not to update records. Currently, there are no options for survey participants to update/correct their PII in the bureaus' records.

(e) Was the minimization of PII in the system considered?

☒Yes ☐No

(f) Does the system use information, including PII, from commercial sources?

☐Yes ☒No

(g) Is the information, including PII, collected from publicly available sources?

☐Yes ☒No

(h) Does the system analyze the PII stored in it?

☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(i) If the system will use test data, will it include real PII?

☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Redress and Notification

(a) Explain whether a notice is provided to the record subject at the point of collection of their information.

Notice is provided to surveys participants who are U.S. Citizens through a Privacy Act statement.

(b) Are opportunities available for record subjects to decline to provide the PII?

☒Yes ☐No

(c) Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?

☐Yes ☒No

(d) What procedures allow record subjects to gain access to their information?

There are two scenarios that address record access procedures. In the first scenario, ECA enables a feature within Qualtrics called 'Anonymize Responses, which severs the link between the respondent's PII (name and email address) and their survey data. This is done intentionally in order to keep the surveys anonymous, thus, ECA cannot locate any particular respondent's record if such a request was made. In the second scenario, ECA asks respondents to voluntarily enter their contact information during the course of the survey. In this scenario, assuming the respondent entered accurate contact information, ECA can locate and provide the records, upon request. Additionally, surveys contain ECA contact email addresses which respondents can reference to request their records from ECA. Note that thus far ECA has not received any inquires or requests of this nature.

(e) Are procedures in place to allow a record subject to correct or amend their information?

☒Yes ☐No

Explain procedures and how record subjects are notified.

As mentioned above in the second scenario of 7d, there are certain surveys that include ECA contact email addresses for respondents to reference if they choose to request their records from ECA. ECA can locate and provide records to respondents for surveys that are included in this scenario.

7. Sharing of PII

(a) To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.

INTERNAL (WITHIN THE DEPARTMENT)	EXTERNAL (OUTSIDE OF THE DEPARTMENT)
N/A	External Contractor (contractors vary) that are involved with the survey Administration.

(b) For each of the entities in 7a, list the PII from 3d that will be transmitted.

INTERNAL (WITHIN THE DEPARTMENT)	EXTERNAL (OUTSIDE OF THE DEPARTMENT)
N/A	Names and Email Addresses

(c) For each of the entities in 7a, what is the purpose for transmitting the information?

INTERNAL (WITHIN THE DEPARTMENT)	EXTERNAL (OUTSIDE OF THE DEPARTMENT)
N/A	The purpose for transmitting the information outside of the Department, to the external contractors, is to provide them with names and email addresses in order for them to follow up with participants if needed and to deploy surveys.

(d) For each of the entities in 7a, list the methods by which the information will be transmitted.

INTERNAL (WITHIN THE DEPARTMENT)	EXTERNAL (OUTSIDE OF THE DEPARTMENT)
N/A	The information is transmitted via password protected excel files; the passwords for these files are sent in a separate email.

(e) For each of the entities in 7a, what safeguards are in place for each method of internal or external transmission?

INTERNAL (WITHIN THE DEPARTMENT)	EXTERNAL (OUTSIDE OF THE DEPARTMENT)
N/A	The information is safeguarded through the use of encrypted emails and password protected excel files. Further, the password of the excel file is shared via a separate email (security practice to prevent packet sniffing attacks).

8. Security

(a) How is all of the information in the system secured?

All of the information in the system is protected in the AWS FedRAMP Gov Cloud. In addition to application-level security controls and inherited security controls of AWS Cloud, the system requires the use of mandatory Multi-Factor Authentication (Okta) to access the system for identification and authentication purposes. This prevents unauthorized users from accessing the data.

(b) Where is the information housed?

FEDRAMP-certified cloud

(c) In the table below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.

ROLE	WHAT DOES THIS ROLE DO?	WHAT PII DOES THIS ROLE HAVE ACCESS TO?	WHAT RIGHTS TO THE PII DOES THE USER HAVE? (READ-ONLY, EDIT, ETC.)	HOW DOES THE ROLE INITIALLY OBTAIN ACCESS?	WHO APPROVES THE ROLE'S ACCESS?
Brand Administrators	Manages account and system configurations; Manages user account settings and permissions; implements policies, process and procedures defined by the ISSO	Names and email for all projects where PII is present.	Read and Edit	This is a privileged account: User first completes the SARF (System Access Request Form); the request is reviewed and approved by the users supervisor, Syst. Owner and ISSO and gets added to the Brand Admins.	Monitoring Evaluation Learning Innovation (MELI) Div. Chief and ISSO
Survey Admin Non-Eval + Editing (General Users)	Design and administer surveys Edit survey responses	PII on projects they created or that are shared with them; mostly names	Read and Edit	User first completes the SARF (System Access Request Form); the request is reviewed and	Monitoring Evaluation Learning Innovation

		and email addresses.		approved by the users supervisor and the Syst. Owner and gets added to the Survey Admin Non-Eval + Editing group.	(MELI) Team and Users Supervisor
Survey Admin Non-Evaluation Division (8eneral Users)	Design and administer surveys; view dashboards.	PII on projects they created or that are shared with them; mostly names and email addresses.	Read and Edit	User first completes the SARF (System Access Request Form); the request is reviewed and approved by the users supervisor and the Syst. Owner and gets added to the Survey Admin Non-Eval group.	Monitoring Evaluation Learning Innovation (MELI) Team and Users Supervisor
Security Administrator	Establishes policies, processes, and procedures in compliance with DoS desktop security guidelines; ensures that security guidelines are followed by the organization.	PII on projects they created or that are shared with them; mostly names and email addresses.	Read only.	This is a privileged account: User first completes the SARF (System Access Request Form); the request is reviewed and approved by the users supervisor, Syst. Owner and ISSO and gets added to the Security Admins.	Monitoring Evaluation Learning Innovation (MELI) Div. Chief and ISSO

(d) After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.

In order to maintain access to the system, the user:

Brand Administrator/ Security Administrator-Privileged account types: Must have their accounts reviewed at least quarterly by the ISSO to ensure that they still need access, must submit a new SARF annually, must complete all mandatory OpenNet trainings (Enterprise users only) and account must be active within the last 90 days.

Survey Admin Non-Evaluation Division/ Survey Admin Non-Eval + Editing- General users: Must have their accounts reviewed at least annually by their supervisor and the system administrator to ensure that they still need access; must submit a new SARF annually; must complete all mandatory OpenNet trainings (Enterprise users only); account must be active within the last 90 days for Enterprise users; 60 days for Non-Enterprise users.

(e) Have monitoring, recording, auditing safeguards, and other controls been put in place to prevent the misuse of the information?

☒Yes ☐No

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Privacy Related Training Certification

- Do all OpenNet users of this system take PA-318 Protecting Personally Identifiable Information biennially?

  ☒Yes ☐No

- Do all OpenNet users of this system take PS800 Cybersecurity Awareness Training annually?

  ☒Yes ☐No

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

  ☐Yes ☒No

  Please list the related trainings here: