Office of Government Ethics

SurveyMonkey
Privacy Impact Assessment

December 2021

Program Counsel Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for SurveyMonkey

Provide electronic copies of the signed PIA to OGE's Chief Information & Cybersecurity Officer and Privacy Officer.

Name of Project/System: SurveyMonkey
Office: Program Counsel Division

Executive Summary

SurveyMonkey is a third-party website and application that enables the agency to create customized surveys. Once a user creates a SurveyMonkey account, the user has access to over 100 survey templates and over 2,500 questions. Users may also create custom templates and questions. SurveyMonkey allows users to send surveys via the internet and email. OGE conducted this PIA because the agency may utilize SurveyMonkey to collect and retain personally identifiable information (PII), including a survey taker's name, address, email address, internet protocol (IP) address, and other information that enables the agency and/or SurveyMonkey to identify respondents. SurveyMonkey's Terms of Service and Privacy Policy govern its collection, use, maintenance, and disclosure of information. It is suggested that users review the SurveyMonkey Privacy Policy before using its services to understand how and when SurveyMonkey collects, uses, and shares the information submitted for OGE surveys using SurveyMonkey's services.

It is intended that this PIA will generally cover OGE's practices regarding the use of SurveyMonkey to generate specific surveys. However, a Privacy Threshold Analysis (PTA) will still be required before a specific survey may be deployed.

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Jennifer Matis
Associate Counsel and Privacy Officer
Legal, External Affairs and Performance Branch
Program Counsel Division
jmatis@oge.gov
202-482-9211

2) Who is the system owner?

Nicole Stein
Chief, Agency Assistance Branch
Program Counsel Division
nstein@oge.gov
202-482-9255

3) Who is the system manager?

Nicole Stein
Chief, Agency Assistance Branch
Program Counsel Division
nstein@oge.gov
202-482-9255

4) Who is the Chief Information Security Officer (CISO) who reviewed this document?

Ty Cooper
Chief Information & Cybersecurity Officer
jtcooper@oge.gov
(202) 482-9226

5) Who is the Senior Agency Official for Privacy who reviewed this document?

Diana J. Veilleux
Senior Agency Official for Privacy
Chief, Legal, External Affairs and Performance Branch
Diana.veilleux@oge.gov
202-482-9203

6) Who is the Reviewing Official?

Ty Cooper
Chief Information & Cybersecurity Officer
jtcooper@oge.gov
202-482-9226

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. Responses to a specific OGE survey generated using the SurveyMonkey application may contain information about individual respondents, depending on the contents of the survey. These individuals may be OGE employees, other federal employees, or members of the public. OGE users also provide basic personal information to the SurveyMonkey application in order to receive administrative access to OGE's account.

a. Is this information identifiable to the individual?

Potentially, based upon the contents of a particular survey.

b. Is the information about individual members of the public?

Potentially, based upon the contents of a particular survey.

c. Is the information about employees?

Potentially.

2) What is the purpose of the system/application?

SurveyMonkey is a third-party website and application that enables the agency to create customized surveys. Surveys are used to gather feedback from agency stakeholders inside or outside OGE.

3) What legal authority authorizes the purchase or development of this system/application?

The specific legal authority varies depending on the purpose of the specific survey being implemented, but may include the Foundations for Evidence-Based Policymaking Act of 2018, Pub.L. No: 115-435 (1/14/2019); Presidential Memorandum on Tribal Consultation and Strengthening Nation-to-Nation Relationships (1/26/2021); and EO 13571, Streamlining Service Delivery and Improving Customer Service (4/27/2011).

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Potentially, OGE employees, other federal employees, and members of the public--depending on the purpose and contents of the survey.

2) What are the sources of the information in the system?

Most of information is collected from the individual themselves. Internet protocol (IP) addresses may be collected directly from the survey taker's computer.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

See above.

b. What federal agencies provide data for use in the system?

Not applicable.

c. What State and local agencies are providing data for use in the system?

Not applicable.

d. From what other third party sources will data be collected?

Not applicable.

e. What information will be collected from the employee and the public?

Information collected from survey takers may contain personally identifiable information (PII), including a survey taker's name, address, email address, and other information.

OGE users must select the option to not collect IP addresses. In the rare case that an OGE user needs IP address information, they must specifically ask for and be granted permission from the Privacy Officer. Such permission will be noted in the review module of the PTA submitted for the specific survey. A screenshot of how to select the option is attached as Attachment A.

3) Accuracy, Timeliness, Reliability, and Completeness

a. How will data collected from sources other than OGE records be verified for accuracy?

Not applicable.

b. How will data be checked for completeness?

Not applicable.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Not applicable. The data is intended to be current when collected and then will be used for historical purposes only.

d. Are the data elements described in detail and documented?

No, however, the data elements are simple and self-explanatory.

D. ATTRIBUTES OF THE DATA:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

   Yes.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

   No.

3) **Will the new data be placed in the individual's record?**

   Not applicable.

4) **Can the system make determinations about employees/the public that would not be possible without the new data?**

   Not applicable.

5) **How will the new data be verified for relevance and accuracy?**

   Not applicable.

6) **If the data is being aggregated, what controls are in place to protect the data from unauthorized access or use?**

   No data is being aggregated.

7) **If data is being aggregated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

   No data is being aggregated.

8) **How will the data be retrieved? Does a personal identifier retrieve the data?**

To the extent that a specific survey collects data that is not anonymized, the data may be retrieved by personal identifier. Whenever a survey will collect data to be retrieved by personal identifier, it must be noted on the Privacy Threshold Analysis (PTA) submitted for the particular survey.

If the Privacy Act will be applicable to the information collected by a particular survey, it must be noted in the review module on the PTA for that survey and the applicable Privacy Act system of records will be cited. To the extent that Privacy Act-protected records are collected and maintained, the survey creator and all other OGE employees accessing the survey information must comply with the Privacy Act and the applicable system of records notice, including posting an appropriate Privacy Act statement within the specific survey.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

To the extent that SurveyMonkey has this capability, OGE users will not avail themselves of that option.

10) **What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)?**

Some of the particular surveys created are voluntary, while some directed at agency employees are required by agency policy. There is no opportunity to consent to particular uses of the information. A Privacy Act statement will be included within any survey that collects Privacy Act-protected records.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Not applicable.

2) **Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?**

Prior to utilizing SurveyMonkey, the survey creator must coordinate with OGE's Records Officer to ensure that the information collected by SurveyMonkey that constitutes "records" under the Federal Records Act, 44 U.S.C. § 3301, will be retained as required by applicable OGE policy and records retention schedules approved by the National Archives and Records Administration (NARA).

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

See above.

4) **Is the system using technologies in ways that the OGE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5) How does the use of this technology affect public/employee privacy?

A specific survey created using SurveyMonkey collects no more information than is necessary and properly secures the information. SurveyMonkey has security protections in place to protect the privacy of its users. See https://www.surveymonkey.com/mp/legal/security/. To the extent that the collected data is maintained on OGE's network, the agency will take appropriate steps to mitigate any potential threats to privacy that exist in light of the survey information collected and shared. OGE will avoid using open text boxes whenever possible to mitigate the possibility of over-collection and will collect only the information necessary for the proper performance of agency functions.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

7) What kinds of information are collected as a function of the monitoring of individuals?

Not applicable.

8) What controls will be used to prevent unauthorized monitoring?

SurveyMonkey does not have the capability to monitor individuals.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

If the Privacy Act will be applicable to the information collected by a particular survey, that must be noted in the review module on the PTA, and the applicable Privacy Act system of records will be cited.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

Not applicable.

F. ACCESS TO DATA:

1) Who will have access to the data in the system?

Only a limited number of OGE users have direct administrative access to SurveyMonkey and to information collected through a particular survey. Only authorized OGE users will have access to the data that is imported into OGE's network through a particular survey. Generally, the information collected will be limited to non-sensitive PII, such as contact information. To the extent individual surveys collect more sensitive PII, the Privacy Officer may impose additional access restrictions on the collected data. Such additional restrictions will be noted in the review module on the specific survey's PTA.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access to OGE applications is governed by the Account Access Request Form (AARF) process, which authorizes the Information Technology Division (ITD) to create, modify, and disable network accounts, including providing access to OGE applications. AARF requests must be signed by the employee, his/her supervisor, and the Chief Information & Cybersecurity Officer before a request is approved to be implemented by ITD staff.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

See above.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

Authorized users have been advised that agency policy prohibits them from unauthorized browsing of data and have been instructed not to engage in such activities.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

No contractors were involved with the design, development, or maintenance of the SurveyMonkey application as utilized by OGE, or any particular surveys.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Not applicable.

8) Will other agencies share data or have access to the data in this system (Federal, State, or Local)?

No.

9) How will the data be used by the other agency?

Not applicable.

10) Who is responsible for assuring proper use of the data?

Each authorized user is responsible for assuring proper use of the data collected via a particular survey.

The Following Officials Have Approved the PIA for SurveyMonkey:

1) **System Manager/Owner**

   Electronic Signature: NICOLE STEIN Digitally signed by NICOLE STEIN Date: 2021.12.14 11:06:51 -05'00'

   Name: Nicole Stein
   Title: Chief, Agency Assistance Branch

2) **Chief Information & Cybersecurity Officer**

   Electronic Signature: JAMES COOPER Digitally signed by JAMES COOPER Date: 2021.12.14 10:50:37 -05'00'

   Name: Ty Cooper
   Title: Chief Information & Cybersecurity Officer

3) **Senior Agency Official for Privacy**

   Electronic Signature: DIANA VEILLEUX Digitally signed by DIANA VEILLEUX Date: 2021.12.14 10:58:29 -05'00'

   Name: Diana Veilleux
   Title: Chief, Legal, External Affairs and Performance Branch and Senior Agency Official for Privacy

Attachment A to OGE PIA for SurveyMonkey

Making Responses Anonymous

The Anonymous Responses collector option lets you choose whether or not to track and store identifiable respondent information in survey results. SurveyMonkey records respondent IP addresses in backend logs and deletes them after 13 months.

Tips for Anonymous Surveys

- If you're using multiple collectors, you need to turn on Anonymous Responses in each collector.
- If you want your survey to be anonymous, don't include identifiable questions in your survey design and don't use identifiable custom data or custom variables when sending your survey.
- If you have an Enterprise plan, Primary Admins can choose a default Anonymous Responses setting for their entire team.

> ⚠ If you need your survey responses to be anonymous, you must turn on the Anonymous Responses setting before you send your survey. It's not possible to make responses anonymous once you've already collected responses.

Web Links

Web Links record the IP addresses of respondents by default.

To turn on Anonymous Responses:

1. Go to the **Collect Responses** section of your survey.
2. Click the name of the collector.
3. Click **Anonymous Responses** and choose **On**.

Email Invitations

Email Invitations are designed to help you track respondents, so your survey results will include the email address and IP address of each respondent by default. Additionally, the first name, last name, and custom data about your contacts is tracked, if you included this information in the collector.

To turn on Anonymous Responses:

1. Go to the **Collect Responses** section of your survey.
2. Click the name of the collector.
3. Go to the collector options. If you've already sent an invitation, go to the **Options** tab. When sending your first invitation message in the collector, you'll choose collector options after composing your message.
4. Click **Anonymous Responses**.
5. Choose to **exclude all respondent information** to exclude first name, last name, email address, IP address, and custom data from your results. Or choose **only exclude personal information** to exclude first name, last name, email address, and IP address from your results.

TIP! Even if Anonymous Responses is turned on, you can still track email invitations. This info is tied to the email invitation, not to survey results.

Facebook Messenger

By default, the Facebook Messenger collector doesn't pass any identifying information to SurveyMonkey, it only passes the survey responses.

Other Collector Types

By default, most collectors record the IP addresses of respondents in survey results. You can turn on Anonymous Responses to prevent IP tracking.

To turn on Anonymous Responses:

1. Go to the collector options for your collector
2. Turn on **Make Anonymous** or turn off **Save IP Address in Results?**

Respondent Authentication

When Respondent Authentication is turned on, the survey is never anonymous because the survey taker’s SSO profile information is tracked.

Collectors Created by Integrations

Some integrations automatically create collectors in SurveyMonkey, like the Microsoft Teams integration. Whether a survey is anonymous or not is dependent on the integration's settings rather than the Anonymous Responses collector option.