U.S. Securities and Exchange Commission

Qualtrics Experience Management (QEM)
PRIVACY IMPACT ASSESSMENT (PIA)

March 29, 2023

Office of Human Resources

Privacy Impact Assessment

Qualtrics Experience Management (QEM)

Section 1: System Overview

1.1 Name of Project or System

Qualtrics Experience Management (QEM)

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally Hosted (Contractor or other agency/organization)

1.3 Reason for completing PIA

☒ New project or system

☐ This is an existing system undergoing an update

First developed:
Last updated:
Description of update:

1.4 Does the system or program employ any of the following technologies?

☐ Enterprise Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☒ Cloud Computing Services

☐ Web Portal

☐ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

Qualtrics Experience Management (QEM) is a Software-as-a-Service (SaaS) survey platform for gathering data from both SEC employees and the public at large (collectively called "respondents"). Surveys are created by SEC staff and respondents complete those surveys online on the Qualtrics platform. Respondent information resides in an Aurora database.

Surveys are categorized as open, anonymous, or confidential. In most cases surveys are distributed anonymously. Open surveys capture the respondent's attribution data (i.e., name, email address, and phone number), anonymous surveys do not. Confidential surveys capture attribution data but it is never reported or disseminated. A confidential survey may have survey metadata associated with the contact list used to distribute the survey. Qualtrics offers multiple products for online data collection: CoreXM, Customer Experience (CustomerXM), Employee Experience, Product Experience, and Brand Experience. At present, SEC is only using CustomerXM and CoreXM.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

44 USC §3501 et seq. (1980) Paperwork Reduction Act (PRA)

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No

☐ Yes

If yes, provide the purpose of collection:
If yes, provide the legal authority:

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No
☐ Yes, a SORN is in progress
☒ Yes, there is an existing SORN
SEC-26 "Mailing, Contact and Other Lists"

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☐ No
☒ Yes

OMB approval under the Paperwork Reduction Act may be required for certain surveys created and distributed through the Qualtrics platform. Some of these surveys will not be considered a "collection of information" as defined under the PRA, including those covered by a statutory exemption in the Securities Act of 1933 for evaluation, and therefore will not be subject to the PRA. If the PRA applies, users may be able to seek OMB approval under the PRA through SEC's Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery, OMB 3235-0731or the Office of the Advocate for Small Business' (OASB) Generic Clearance, OMB 3235-0787.

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

Given that QEM is used for conducting surveys using text boxes, there is the risk of PII being included in the information collected from surveys. To mitigate this risk, SEC staff using QEM trained to provide warnings to users against providing PII in their responses, if the survey is using free form text boxes for responses.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☐ Social Security Number	☐ Alien Registration	☐ Financial Accounts
☐ Taxpayer ID	☐ Driver's License Number	☐ Financial Transactions
☐ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☐ File/Case ID	☐ Credit Card Number	☐ Employer ID
☐ Other:		

General Personal Data

☒ Name	☒ Date of Birth	☐ Marriage Records
☐ Maiden Name	☒ Place of Birth	☒ Financial Information
☐ Alias	☒ Home Address	☐ Medical Information
☒ Gender	☒ Telephone Number	☒ Military Service
☒ Age	☒ Email Address	☐ Mother's Maiden Name
☒ Race/Ethnicity	☒ Education Records	☐ Health Plan Numbers
☐ Civil or Criminal History	☒ Zip Code	

☒ Other: LGBTQ+ status, whether located in or investing in a rural community and/or an area recently impacted by natural disasters. Additional personal identifiers not explicitly listed above and collected by QEM may be provided by respondents in open text fields responses and used to retrieve additional personal information.

Work-Related Data

☒ Occupation	☒ Telephone Number	☒ Salary
☒ Job Title	☒ Email Address	☒ Work History
☒ Work Address	☐ Certificate/License Number	☒ Business Associates
☐ PIV Card Information	☐ Fax Number	

☒ Other: Supervisory status, office, grade, pay plan, occupational series. Additional personal identifiers not explicitly listed above and collected by QEM may be provided by respondents in open text fields responses and used to retrieve additional personal information.

Distinguishing Features/Biometrics

☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature

☐ Other:

System Administration/Audit Data

☒ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☒ IP Address	☐ Queries Ran	☐ Contents of Files

☒ Other: City and state geographic information.

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

PII may be collected, used, shared, or maintained as a result of survey responses.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees

Purpose: The purpose is dependent on the business needs of the SEC Division/Office. Existing examples include use with contacting the Help Desk for troubleshooting issues or for Human Resources purposes.

☒ SEC Federal Contractors

Purpose: Same as SEC Employees.

☒ Interns

Purpose: Same as SEC Employees.

☒ Members of the Public

Purpose: Purpose is dependent on the business needs of the SEC Division/Office. Existing examples include surveys to evaluate investor education programs, collect information about respondents' views of SEC activities, including information from small businesses and their investors to understand these populations and their roles in the small business ecosystem.

☐ Employee Family Members

Purpose:

☐ Former Employees

Purpose:

☒ Job Applicants

Purpose: The purpose is dependent on the business needs of the SEC Division/Office. Existing examples include surveys to gather contact information, general educational enrollment information, and job preferences in order to target outreach regarding upcoming events and/or job opportunities at the SEC.

☐ Vendors

Purpose:

☐ Other:

Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

The collection of PII is minimized in the surveys through the use of check boxes, radio options, and drop down entries wherever possible, limiting the number of open text boxes. Anonymous surveys do not collect attribution data. These surveys are delivered using a common web link for all respondents or, if delivering to an email address via unique link, use the anonymized responses feature which strips the email information and will not append any metadata. These surveys capture only the information provided in the surveys responses. PII in the system is not used for testing, training, or research efforts.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☐ No.

☒ Yes. General Records Schedule (GRS) 3.1-011, "General Technology Management Records - System Development Records" DAA-GRS-2013-0005-0007

3.6 What are the procedures for identification and disposition at the end of the retention period?

Records will be destroyed 5 years after it is no longer need, however longer retention is authorized under the schedule if required for business use.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A

☐ Members of the Public
Purpose:

☐ Employees
Purpose:

☐ Contractors
Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The data collected 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. QEM surveys are intended to be anonymous. However, there may be survey questions that could be used to parse responses where a single individual could be identified. This privacy risk is mitigated by implementing access controls that limit survey access only to the survey administrator with a business need-to-know.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☐ Privacy Act Statement

☒ System of Records Notice

SORN SEC-26 Mailing, Contact and Other Lists is not provided to individuals prior to collection, but is published in the Federal Register and is available on the SEC's website www.sec.gov.
85 FR 85440 (January 27, 2021)

☒ Privacy Impact Assessment
The QEM PIA is not provided to individuals prior to collection, but is published on the SEC's website, www.sec.gov.
Date of Last Update:

☐ Web Privacy Policy

☐ Other notice:

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

The privacy risk identified is that the individual may not be aware of how their collected information is being used prior to them consenting to the use of their information. This risk is mitigated by requiring requests to administer surveys to align with SEC's internal policy for collecting and protecting Personally Identifiable Information (PII). This risk is also mitigated by the publishing of SORN SEC-26, which authorizes the collection of information; and this PIA which provides adequate notice to individuals regarding information collection purpose and use.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

QEM offers built-in functionality to run analyses on the data collected to gain a deeper understanding of issues that are of interest to SEC. Survey responses are exported by SEC Survey Administrators into a variety of formats, including Word, Excel, Portable Document Format (PDF), extensible markup language (XML), and HyperText Markup Language (HTML). Survey analyses would be dependent on the business needs of the SEC Division or Office, however no new information on the respondents is generated.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes
Organizations: All SEC offices/divisions may distribute a survey. Only the survey administrator of the office or division that distributes a survey will have access to the data.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

There is a risk of inadvertent disclosure of PII to SEC personnel who do not have a need-to-know. This risk is mitigated because survey information is available to only the platform Brand Administrator and the Survey Owner. In addition, surveys have optional capabilities to password protect a survey if sensitive information is requested.

5.4 Will external organizations have access to the data?

☒ No
☐ Yes
Organizations:

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

There is no risk to privacy as data is not shared externally.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☒ Directly from the individual.
☐ Other source(s):

6.2 What methods will be used to collect the data?

Data is collected directly from individuals through the use of an internet browser web interface and stored at Qualtrics on the AWS Gov Cloud.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

Data collected from individuals is manually reviewed by survey administrators. Additionally, survey admins can manage the validation rules for data entry fields in the survey.

6.4 Does the project or system process, or access, PII in any other SEC system?

☒ No
☐ Yes.
System(s):

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

There is a risk for incomplete or inaccurate information that can lead to incorrectly informed decisions. This risk is mitigated as described in Section 6.3.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Participation is voluntary and consent to a survey is limited to a particular survey. Individuals must provide specific consent for each survey for which they are a respondent.

7.2 What procedures are in place to allow individuals to access their information?

Individuals can not directly access their information once entered in the survey. However, individuals may contact the survey administrator listed in the point of contact information provided in the survey invitation email. Additionally, individuals may submit a FOIA request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736 or email request to foiapa@sec.gov.

7.3 Can individuals amend information about themselves in the system? If so, how?

In general, individuals cannot amend information about themselves once entered in the survey. However a survey may be configured to "always on" to enable respondents to login and make updates to their information.

QEM administrators may also delete information associated with an individual's unique identifier upon request. Additionally, individuals may submit a FOIA request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-2736 or email request to foiapa@sec.gov.

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

The primary risks are lack of access to information and inability to seek redress and correction. This risk is mitigated as individual participation is voluntary and the participants directly provide the information with the assumption being that the information is accurate. In addition, respondents may submit a request to the address in 7.2.

Section 8: Security

8.1 Can the system be accessed outside of a connected SEC network?

☐ No
☒ Yes

If yes, is secured authentication required?	☐	No	☒	Yes	☐	Not Applicable
Is the session encrypted?	☐	No	☒	Yes	☐	Not Applicable

8.2 Does the project or system involve an online collection of personal data?

☒ No
☐ Yes

Public
URL:

8.3 Does the site have a posted privacy notice?

☒ No
☐ Yes
☐ N/A

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC staff and contractors receive initial and annual privacy awareness training, which outlines roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security responsibilities and how to fulfill them.

9.2 Does the system generate reports that contain information on individuals?

☐ No
☒ Yes

Audit reports contain name and username for individuals.

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☒ No
☐ Yes
☐ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No

☒ Yes

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

A residual risk related to access, given the sensitivity of the PII in the system, can include the inadvertent handling or misuse of data. To mitigate this risk, role-based access controls limit access to respondent data to only authorized SEC staff with a business need-to-know.