



Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 425
System Name: XM Discover
CPO Approval Date: 5/8/2023
PIA Expiration Date: 5/7/2024

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
XM Discover

B: System, application, or project includes information about:
Federal Employees, Contractors and Public

MRAS collects RFI responses which can and oftentimes do contain sensitive information. We also collect sensitive, demographic info (email address, race, gender, ethnicity, etc) and employee information reports to IG.

C: For the categories listed above, how many records are there for each?

1,393 Records

D: System, application, or project includes these data elements:

Business email address, race, gender, ethnicity, etc) and employee information reports to IG. First Name, Last Name, Email address, Phone number, Job Title, Agency, Location (City, State), Building Number

1. **Contact Information:** Full Name, work and personal email address, work and personal phone number.
2. **Demographic Information:** GS Level, Supervisory Status and Employment details, race, gender, disability status, etc.
3. **Business Information:** Company Name, Contract Number and other Federal Acquisition Services (FAS) related details, NAICS Code, etc. Building Information from Public Buildings Service (PBS)
4. **Device or Software Based Information:** IP Address, Device Type, Web Application, Version, Screen Resolution, Flash version, Java support, user agent, Websites, URLs, Browser Type, Operating System
5. **Platform:** Google Analytics sites

Overview:

XM Discover is a natural language processing add-on to Qualtrics, GSA's enterprise customer experience management platform. XM Discover ingests survey data from Qualtrics and applies sentiment and topic analysis models to analyze themes in open-text feedback. MRAS collects RFI responses which can and oftentimes do contain sensitive information. We also collect sensitive, demographic info (email address, race, gender, ethnicity, etc) and employee information reports to IG.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information? Per [GSA Order 5460.1](#) OCE GSA Customer/Supplier Surveys. Purpose: This Order establishes and communicates new policy regarding the General Services Administration's (GSA) survey initiatives. GSA's Office of Customer Experience (OCE) is responsible for embedding customer-oriented thinking into GSA's daily operations to ensure GSA delivers great customer experiences in addition to great products and services. This Order designates OCE as the official entity responsible for ensuring survey materials distributed to recipients outside of GSA and/or across all of GSA meet agency standards. The observation of this policy will reduce the burden to our customers and promote data transparency into survey results. This will allow GSA to better realize efficiencies around survey administration and standardize survey practices, as measured by OCE across GSA.

In addition, Qualtrics XM Discover is authorized by 5 U.S.C. 301, 40 U.S.C. 121, 40 U.S.C. 582, 40 U.S.C. 3101, 40 U.S.C. 11315, 44 U.S.C. 3602, E.O. 9397, as amended, and Homeland Security Presidential Directive 12 (HSPD-12).

See the links below:

1. GSA Order 5460.1: <https://insite.gsa.gov/directives-library/gsa-customer-supplier-surveys-54601-oce>
2. Paperwork Reduction Act: <https://pra.digital.gov/>
3. Section 508 of the Rehabilitation Act: <https://www.section508.gov/>

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?

Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?

Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?

The following SORNS apply: GSA/CIO-1, and GSA/GOVT-9

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.

Records related to acquiring customers' feedback through survey instruments, comment forms, correspondence, and non-written communications. Customer Survey Questionnaire, Focus Group, and Interview Files. Records related to developing, administering, evaluating, and reporting on customer feedback in the forms of survey questionnaires, focus groups, and telephone/in-person interviews. a. Case files related to developing, administering, and evaluating the effectiveness of questionnaires, focus groups, and telephone/in-person interviews. Included are: · Drafts and final versions of information collection instrument, such as: · Survey questionnaire, · Prepared script for focus group, and/or · Set of questions for telephone/in-person interviews); · E-mails, other correspondence, and comments; · Records related to the OMB clearance process, such as; · OMB Form 83-1, Paperwork Reduction Act Submission, and · Supporting statement (for information collection); · Agreements and contractual documents, such as: · Statements of work, · Requisitions · Purchase orders, and · Requisitions · Instructions and other documents regarding administration of information collection instrument; · Evaluations of instrument's effectiveness; and · Other related records. (1) Files maintained by office(s) responsible for conducting questionnaires, focus groups, and interviews.

Temporary N01-0064-2000-0008 Item 8a Cut off upon completion of administration of questionnaire, focus group, or telephone/in person interviews. Destroy when 6 years old. (N1-64-00-8, item 8a)

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?

The information collected is necessary to meet the follow:

- The Office of Management and Budget (OMB)/ GSA Office of Mission Assurance Guidance M-05-24 for Homeland Security Presidential Directive (HSPD)-12 which authorizes Federal departments and agencies to ensure that contractors have limited/controlled access to facilities and information systems, and
- GSA Directive CIO P 2181.1 Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing which states that GSA contractors must undergo a minimum of a FBI National Criminal Information Check (NCIC) to receive unescorted physical access
- Post-Event/Training Purposes- for Feedback
- Evaluating Employee Satisfaction Levels
- Event Registration Purposes
- Market Research as a Service (MRAS)- is an office within FAS's Customer & Stakeholder Engagement (CASE) Division, which collects Request Information Responses (RFI) which contains sensitive information.

3.2: Will the system, application, or project create or aggregate new data about the individual?

No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

Only Role Based Access control has been implemented to all authorized users. All system users are GSA employees and are considered internal users. There are no users external to GSA. All users have their employee status categorized with a sensitivity level and authenticate using SecureAuth/SSO. In addition, sensitive data are encrypted both at rest and in transit using the AES-256 and TLS1.2 protocols.

3.4 Will the system monitor the public, GSA employees, or contractors?

None

3.4 Explain: Please elaborate as needed.

None. XM Discover does not monitor users. It is only used for collecting survey responses.

3.5 What kinds of report(s) can be produced on individuals?

Reports can not be produced on individuals.

3.6 Will the data included in any report(s) be de-identified?

Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

The process is to delete the field from the report.

3.6 Why Not: Why will the data not be de-identified?

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?

Federal Agencies

4.2How: If so, how will GSA share the information?

Data is shared with the Office of Management and Budget (OMB).

4.3: Is the information collected:

Directly from the Individual

4.3Other Source: What is the other source(s)?

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?

Yes

4.4WhoHow: If so, who and how?

The Qualtrics Insight Platform interconnects with Salesforce and Tableau. The system has the capability to transmit any data to any GSA system via API, but an additional IT security process is already in place for API users. Integrations with GSA systems are built on a project-by-project basis. Current integrations include: transmitting survey responses to Salesforce, leveraging RPA to automate workflows with multiple forms/surveys and populate spreadsheets and documents, pulling response datasets from Qualtrics to Tableau Desktop for visualization.

4.4 Formal Agreement: Is a formal agreement(s) in place?

No

4.4 No Agreement: Why is there not a formal agreement in place?

Interconnection Security Agreement (ISA) is not required because both systems are under the same Authorizing Official (AO).

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

XM Discover is a survey tool and requires that survey respondents provide accurate information for completeness. Once information entered is submitted, survey respondents have no opportunity to amend the information they have provided.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

OCE's Voice of the Customer (VoC) Program Team Members are the brand administrators in Qualtrics. They have an ability to view all survey data in the platform. These are classified as privileged users. Brand Administrators have the ability to proxy into any account at any time, only with the permission of the account holder or the supervisor.

GSA employees, also known as "Regular Users" and/or "License/Account Holders" can only view survey data for surveys they create. They cannot view surveys of other users. However, users can export their surveys and share (or " collaborate") with other team members or export survey questions and survey data to be shared with colleagues.

6.1b: What is the authorization process to gain access?

Brand Administrators are given access by their Office of Customer Experience (OCE) supervisor. An existing Brand Administrator is authorized to create a new account for the Brand Administrator.

GSA end users request are able to request an account via email to the Office of Customer Experience (OCE) brand administrators with their name, email address, office and business justification. The Office of Customer Experience (OCE) Brand Administrators will verify their need for access and create the new user account.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?

No

6.2a: Enter the actual or expected ATO date from the associated authorization package.

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?

Role based access control (RBAC) are implemented. End users login via SecureAuth SSO. Users are also given a brand ID for access.

Brand Administrators are given separate user account from their end user account to perform admin duties. They login with a PIN and SNA token.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?

Yes

6.4 What: What are they?

XM Discover Program and Technical Teams will follow the Incident Response processes and procedures detailed in the GSA IT Procedural Guide: Incident Response (IR) CIO-IT Security-01-02. In addition incidents will be reported to the vendor.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?

There is an opportunity for individuals to respond to or decline to surveys. Surveys are voluntary and Individuals do not have to respond.

7.1Opt: Can they opt-in or opt-out?

Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that allow individuals to access their information?

There are no procedures in place to allow individuals to access their information. Once information is submitted, it marked as final and only the Brand Administrators can see user's information.

7.3: Can individuals amend information about themselves?

No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

All GSA employees and contractors are required to complete the GSA provided Security and Privacy Awareness Training during on boarding and annually thereafter. GSA requires annual privacy and security training for all personnel and has policies in place that govern the proper handling of PII. This is managed through the CIO and Online Learning University system (GSA OLU).

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?

The OCE team has access to all of the data that is captured. Users of the system are able to share information. The OCE team entrust end users with the responsibility to share their survey responses with persons they have determined to have the need to know. Also, GSA requires privacy and security training for all personnel, and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, including those that support design research, and has limited access to those personnel with a need to know. Further, OMB requires GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. additionally, GSA takes automated precautions against overly open access controls.
