

**U.S. Department of Commerce
U.S. Census Bureau**



**Privacy Threshold Analysis
for the
Qualtrics,
Cloud Based Survey Software**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau, Qualtrics

Unique Project Identifier: [Number]

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

The Census Bureau's use of the Qualtrics system will sever two separate and distinct purposes:

1. The Census Bureau's Center for Behavioral Science Methods (CBSM) employs a variety of qualitative research methods, including cognitive interviews, usability testing and focus groups to test new materials and methods as well as to understand public perceptions of the work the Census Bureau is doing.
2. In addition, the Census Bureau may conduct ad-hoc surveys through the CBSM to measure certain social and economic conditions of the nation. CBSM uses a cloud-based subscription survey software to allow for online collection of information to support Census Bureau activities. The sampling frame is taken from the Census Bureau's Master Address File (MAF). Introductory notices and reminders to complete the survey will be sent to survey respondents by email or text message (depending on what is available in the Census MAF).

Survey information collected in this system is used for statistical purposes only. Personally identifiable information (PII) collected in this system by CBSM is protected from unauthorized disclosure, under Title 13, U.S.C., and can only be used by sworn Census Bureau employees or contractors in support of our data collection efforts. The Qualtrics cloud service provider does not have access to the encryption keys of Census data.

(a) Whether it is a general support system, major application, or other type of system

Other – software as a service, research tool

(b) System location

Amazon Gov Cloud located in Oregon, U.S.A.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Stand-alone

(d) The purpose that the system is designed to serve

Research information for developing and testing questionnaires will be used by staff from the Census Bureau to evaluate and improve the quality of the data in the surveys and censuses that are ultimately conducted.

Information collected for survey data will be used to produce national demographic and economic statistics.

(e) The way the system operates to achieve the purpose(s) identified in Section 4

This system will serve as a research data collection tool. In addition to collecting data, the tool is also used to evaluate and improve the Census Bureau's online services for decennial, economic and demographic surveys. The tool is programmed by Census Bureau staff and sent to sampled members of the public, employees or customers for data collection. Through this tool, the Census Bureau is able to:

- Create, test, modify, and implement surveys
- Apply flow logic to surveys with advanced branching and display logic,
- Use a variety of question types,
- Embed data (either pre-existing from an input file or from previous survey questions),
- Ability to implement survey quotas,
- Mobile and offline compatibility,
- Randomization within question, between questions and between survey instruments.

(f) A general description of the type of information collected, maintained, use, or disseminated by the system

The types of information that will be used by Qualtrics is General Personal Data and Work Related Data PII. The information collected in this program of developing and testing questionnaires will be used by staff from the Census Bureau to evaluate and improve the quality of the data in the surveys and censuses that are ultimately conducted.

(g) Identify individuals that have access to the system.

The general public will have access to enter their own data only; they will not have access to other respondents' data. Only government employees and contractors will have access to other respondent's data.

(h) How information in the system is retrieved by the user

Data access depends on user type. If the user has access to the data, they can retrieve the data based on any of the characteristics collected in the data, including personally identifiable information (PII).

(i) How information is transmitted to and from the system

Respondents submit data using HTTPS (TLSv1.2 with AES 128/256 depending on the browser) to the front-end web server (typically *customername.qualtrics.com*). All data in transit (respondent data to the cloud and the data from the cloud to Census) is encrypted via TLSv1.2.

Data are processed by application servers and sent to database servers for storage. Web data are delivered to the respondent in the form of survey questions, graphics, and other content created in the survey design. Some surveys are restricted by password or location, as setup by the survey creator. This multi-tiered architecture has multiple layers of hardware and software security to ensure that no device/user can be inserted into the communication channel.

For high availability and speed, base code and static images/docs are stored in the cloud and delivered to Users as efficiently as possible using cache and location information.

Users access the Qualtrics platform with login credentials using a web browser. Customers may choose to authenticate by linking their single sign-on (SSO) system to Qualtrics' Services. Brand Administrators have full control over Users and the password policy.

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): This system will also be used for conducting ad-hoc surveys on a sample of the public to measure the social and economic conditions of the nation.			

This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015). *Continue to answer questions and complete certification.*

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII.

No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to 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."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

National Institute of Standards and Technology Associates

Contractors working on behalf of DOC

Other Federal Government personnel

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to Qualtrics and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Jennifer Hunter Childs

Signature of SO: JENNIFER CHILDS Digitally signed by JENNIFER CHILDS
Date: 2020.05.06 12:46:23 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Beau Houser

Signature of CISO: BEAU HOUSER Digitally signed by BEAU HOUSER
Date: 2020.05.20 13:32:54 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: BYRON CRENSHAW Digitally signed by BYRON
CRENSHAW
Date: 2020.05.29 10:37:51 -04'00' Date: _____

Name of Authorizing Official (AO): Kevin Smith

Signature of AO: KEVIN SMITH Digitally signed by KEVIN SMITH
Date: 2020.07.16 15:24:17 -04'00' Date: _____

Name of Authorizing Official (AO): John Eltinge,
Robert Sienkiewicz is Acting for John Eltinge and signs on his behalf.

Signature of AO: ROBERT SIENKIEWICZ Digitally signed by ROBERT
SIENKIEWICZ
Date: 2020.07.01 18:19:30 -04'00' Date: _____

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: BYRON CRENSHAW Digitally signed by BYRON
CRENSHAW
Date: 2020.05.29 10:38:22 -04'00' Date: _____