Version Number: 01-2017

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

## Privacy Impact Assessment
## for the
## Qualtrics,
## Cloud Based Survey Software

Reviewed by: 4/19/18, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.11.09 13:48:28 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

# U.S. Department of Commerce Privacy Impact Assessment
# 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 Center for Survey Measurement (CSM) 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. CSM needs a cloud-based subscription survey software to allow for collection of information to support CSM activities.

The contractor must provide a subscription to the cloud-based subscription survey software for five (5) Census Bureau users and allow for up to 50,000 responses (cumulative) for one year.

The Census Bureau may have a need to increase the number of users/seats and the number of responses to be collected. The contractor may propose pricing for additional users/seats and an increased number of responses (optional service).

*(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

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

This system will serve as a research data collection tool to evaluate and improve the Census Bureau's online services for decennial and demographic surveys. The tool will be programed by Census Bureau staff and sent to sampled members of the public, employees or customers for data collection. We will be able to:

- Create, test, and modify 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.

*(e) 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.

*(f) 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.

*(g) Any information sharing conducted by the system*

Data collected in this system will be stored within the system and transferred to Census Bureau systems for storage and analysis as described above.

*(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

Title 13 U.S.C., Sections 6 (c), 141 and 193
Title 13 U.S.C. 8(b), 182, and 196.
15 CFR part 50.

*(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Medium

## Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

__X__ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

| 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 is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

## Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

| Identifying Numbers (IN) | | | | | |
|---|---|---|---|---|---|
| a. Social Security* | | e. File/Case ID | | i. Credit Card | |
| b. Taxpayer ID | | f. Driver's License | | j. Financial Account | |
| c. Employer ID | | g. Passport | | k. Financial Transaction | |
| d. Employee ID | | h. Alien Registration | | l. Vehicle Identifier | |
| m. Other identifying numbers (specify): | | | | | |
| *Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: | | | | | |

| General Personal Data (GPD) | | | | | |
|---|---|---|---|---|---|
| a. Name | X | g. Date of Birth | X | m. Religion | |
| b. Maiden Name | X | h. Place of Birth | X | n. Financial Information | |
| c. Alias | X | i. Home Address | X | o. Medical Information | |
| d. Gender | X | j. Telephone Number | X | p. Military Service | x |
| e. Age | X | k. Email Address | X | q. Physical Characteristics | |
| f. Race/Ethnicity | X | l. Education | X | r. Mother's Maiden Name | |
| s. Other general personal data (specify): | | | | | |

| **Work-Related Data (WRD)** | | | | | |
|---|---|---|---|---|---|
| a. Occupation | X | d. Telephone Number | X | g. Salary | X |
| b. Job Title | X | e. Email Address | X | h. Work History | X |
| c. Work Address | X | f. Business Associates | | | |
| i. Other work-related data (specify): | | | | | |

| **Distinguishing Features/Biometrics (DFB)** | | | | | |
|---|---|---|---|---|---|
| a. Fingerprints | | d. Photographs | | g. DNA Profiles | |
| b. Palm Prints | | e. Scars, Marks, Tattoos | | h. Retina/Iris Scans | |
| c. Voice Recording/Signatures | | f. Vascular Scan | | i. Dental Profile | |
| j. Other distinguishing features/biometrics (specify): | | | | | |

| **System Administration/Audit Data (SAAD)** | | | | | |
|---|---|---|---|---|---|
| a. User ID | X | c. Date/Time of Access | X | e. ID Files Accessed | |
| b. IP Address | X | d. Queries Run | | f. Contents of Files | |
| g. Other system administration/audit data (specify): | | | | | |

| **Other Information (specify)** |
|---|
| |
| |

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

| **Directly from Individual about Whom the Information Pertains** | | | | | |
|---|---|---|---|---|---|
| In Person | | Hard Copy: Mail/Fax | | Online | X |
| Telephone | | Email | | | |
| Other (specify): | | | | | |

| **Government Sources** | | | | | |
|---|---|---|---|---|---|
| Within the Bureau | | Other DOC Bureaus | | Other Federal Agencies | |
| State, Local, Tribal | | Foreign | | | |
| Other (specify): | | | | | |

| **Non-government Sources** | | | | | |
|---|---|---|---|---|---|
| Public Organizations | | Private Sector | | Commercial Data Brokers | |
| Third Party Website or Application | | | | | |
| Other (specify): | | | | | |

2.3 Describe how the accuracy of the information in the system is ensured.

| |
|---|
| 1. A respondent takes a survey and the response is submitted to Qualtrics short-term response storage over HTTPS.<br>**2** The unique customer ID for the survey is referenced to determine whether or not the customer uses Qualtrics Data Isolation. If the customer uses Data Isolation, all data for every survey collected by that customer are encrypted.<br>**3** If Data Isolation is used, the Encryption Service uses the customer-specific Master Key in Amazon KMS service to retrieve the survey's AES 256-bit data encryption key from the Amazon Key Management Service.<br>**4** The Encryption Service uses the key, plus a response-specific initialization vector, to encrypt the data and write it to the Qualtrics Response Database.<br>**5** When the response information is eventually recorded to backup in an offsite data center, backup data are still in its encrypted form and an extra layer of encryption is applied to the entire disc.<br><br>**1** The user authenticates to Qualtrics.<br>**2** The user makes a request to response storage to get data for a particular survey.<br>**3** The unique customer ID for the survey is referenced to determine whether or not the customer uses Qualtrics Data Isolation.<br>**4** If Data Isolation is used, the Encryption Service uses the customer-specific Master Key in Amazon KMS service to retrieve the survey's AES 256-bit data encryption key from the Amazon Key Management Service.<br>**5** The encrypted data are retrieved from the Qualtrics Response Cache and/or Response Database and then decrypted with the customer's key and the response's unique initialization vector.<br>**6** The data are returned in plaintext to the user over HTTPS. |

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| X | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection.<br>0607-0725; 0607-0978; 0607-0971 |
| | No, the information is not covered by the Paperwork Reduction Act. |

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

| **Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)** | | | |
|---|---|---|---|
| Smart Cards | | Biometrics | |
| Caller-ID | | Personal Identity Verification (PIV) Cards | |
| Other (specify): | | | |

| | |
|---|---|
| X | There are not any technologies used that contain PII/BII in ways that have not been previously deployed. |

## Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

| | |
|---|---|
| X | There are not any IT system supported activities which raise privacy risks/concerns. |

## Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

| **Purpose** | | | |
|---|---|---|---|
| For a Computer Matching Program | | For administering human resources programs | |
| For administrative matters | | To promote information sharing initiatives | |
| For litigation | | For criminal law enforcement activities | |
| For civil enforcement activities | | For intelligence activities | |
| To improve Federal services online | X | For employee or customer satisfaction | X |
| For web measurement and customization technologies (single-session ) | | For web measurement and customization technologies (multi-session ) | |
| Other (specify): The information being collected will be used to support the Center for Survey Measurement (CSM) in testing new materials and methods to understand public perceptions of the work the Census Bureau is doing. This will be used in addition to the qualitative research methods, cognitive interviews, usability testing and focus groups that CSM currently conducts. | | | |

## Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII will be collected from members of the public.

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.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

| |
|---|
| All system users will complete annual Data Stewardship Training and will sign both the Census Bureau and the Qualtrics' Acceptable Use Policies, which specify the protection of data, and that the data, when applicable, is stored on the secure Census network.<br><br>All data in transit (respondent data to the cloud and the data from the cloud to Census) is encrypted via TLSv1.2.<br><br>Deprecated or defective media (specifically, hard drives) are erased according to a U.S. Department of Defense compliant 3-pass overwrite standard, and/or physically destroyed.<br><br>At the end of the retention period, surveys will be deleted. Since Qualtrics uses the data isolation service, a key hierarchy is created for each Federal customer. Key management is via Amazon Web Services Key Management Service (KMS). Each customer has a unique Key Encryption Key (KEK) used to encrypt and protect a series of unique Data Encryption Keys (DEK). A unique DEK is created for each customer survey. A federal customer may request key destruction of the customer specific KEK which leads to survey data destruction. The data decommissioning procedures are established by the federal customer Brand administrator. |

## Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

| Recipient | How Information will be Shared | | |
|---|---|---|---|
| | Case-by-Case | Bulk Transfer | Direct Access |
| Within the bureau | | X | X |
| DOC bureaus | | | |
| Federal agencies | | | |
| State, local, tribal gov't agencies | | | |
| Public | | | |
| Private sector | | | |
| Foreign governments | | | |
| Foreign entities | | | |
| Other (specify): | | | |

| | |
|---|---|
| | The PII/BII in the system will not be shared. |

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

| | |
|---|---|
| | Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: |
| X | No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. |

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

| **Class of Users** | | | |
|---|---|---|---|
| General Public | X | Government Employees | X |
| Contractors | X | | |
| Other (specify): General public will have access to enter their own data only. They will not have access to other respondents' data. The contractor will provide access to five (5) Census Bureau users for the purpose of programming multiple surveys and collecting up to 50,000 responses for one year. General public access is for input only. | | | |

## Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

| | | |
|---|---|---|
| | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. | |
| X | Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: A notice specific to the collection will be provided by a Privacy Act statement once the user accesses the system. | |
| | Yes, notice is provided by other means. | Specify how: |
| | No, notice is not provided. | Specify why not: |

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to decline to provide PII/BII. | Specify how: Individuals may refuse to participate in the survey or, if they do participate, they may refuse to answer specific questions. |
| | No, individuals do not have an opportunity to decline to provide PII/BII. | Specify why not: |

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to consent to particular uses of their PII/BII. | Specify how: The privacy act statement will provide informed consent specific to each data collection. |
| | No, individuals do not have an opportunity to consent to particular uses of their PII/BII. | Specify why not: |

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

| | | |
|---|---|---|
| | Yes, individuals have an opportunity to review/update PII/BII pertaining to them. | Specify how: |
| X | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not: These data are collected for research purposes only, therefore there is not an opportunity to review/update. |

## Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

| | |
|---|---|
| X | All users signed a confidentiality agreement or non-disclosure agreement. |
| X | All users are subject to a Code of Conduct that includes the requirement for confidentiality. |
| X | Staff (employees and contractors) received training on privacy and confidentiality policies and practices. |
| X | Access to the PII/BII is restricted to authorized personnel only. |
| X | Access to the PII/BII is being monitored, tracked, or recorded.<br>Explanation: |
| | The information is secured in accordance with FISMA requirements.<br>Provide date of most recent Assessment and Authorization (A&A): _____<br>☒ This is a new system. The A&A date will be provided when the A&A package is approved. |
| X | The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. |
| X | NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M). |
| X | A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks. |
| X | Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy. |
| X | Contracts with customers establish ownership rights over data including PII/BII. |
| X | Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers. |
| | Other (specify): |

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

| |
|---|
| All response data resides in Amazon Web Services (AWS) GovCloud (environment is specific only for Federal customers), and data is protected by disk level encryption and database encryption. AWS GovCloud has an existing ATO (Authority to Operate) under FedRAMP, which gives Government agencies the ability to leverage AWS GovCloud for sensitive workloads.<br><br>Privileged Engineer access to the Insight Platform production environment is by SSH to the bastion host, but they do not have access to customer PII. Within the production system, Qualtrics uses both disk level encryption as well as database encryption to protect customer data.<br><br>Qualtrics uses Transport Layer Security (TLS) encryption for all transmitted Internet data. Customers may opt to password protect their surveys, or have unique ID links that are difficult to guess. Our services are hosted by trusted third party data centers that are audited using the industry standard SSAE-16 SOC 1 Type 2 method. All data at rest are protected using sophisticated electronic controls, and data on deprecated hard drives are destroyed by U.S. DOD methods and delivered to a third-party data destruction service. The Qualtrics Security and Privacy Officer is accredited by ISC2 and IAPP (CIPP/US). |

## Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

| | |
|---|---|
| | Yes, this system is covered by an existing system of records notice (SORN).<br>Provide the SORN name, number, and link. *(list all that apply)*: |
| X | Yes, a SORN has been submitted to the Department for approval on (date).<br><br>CENSUS-3: (New Proposed Name: Demographic Survey Collection (Census Bureau Sampling Frame)) - http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html<br><br>CENSUS-5: Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html<br><br>CENSUS-7: (New Proposed Name: Demographic Survey Collection (non-Census Bureau Sampling Frame))- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html |
| | No, this system is not a system of records and a SORN is not applicable. |

## Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

| | |
|---|---|
| X | There is an approved record control schedule.<br>Provide the name of the record control schedule: |

| | |
|---|---|
| | GRS 3.1<br>GRS 4.2<br>Decennial Records are covered by:<br>Nl-29-05-01, N1-29-10-5, GRS 3.1, GRS 5.6 item 181<br>Demographic Records are covered by:<br>N1-29-99-5, N1-29-89-3, N1-29-87-3, N1-29-86-3, NC1-29-85-1, NC1-29-79-7, and GRS 3.1 GRS 3.2 GRS 4.1, GRS 4.3 |
| | No, there is not an approved record control schedule.<br>Provide the stage in which the project is in developing and submitting a records control schedule: |
| X | Yes, retention is monitored for compliance to the schedule. |
| | No, retention is not monitored for compliance to the schedule. Provide explanation: |

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

| **Disposal** | | | |
|---|---|---|---|
| Shredding | | Overwriting | |
| Degaussing | | Deleting | X |
| Other (specify): At the end of the retention period, surveys will be deleted. Since Qualtrics uses the data isolation service, a key hierarchy is created for each Federal customer. Key management is via Amazon Web Services Key Management Service (KMS). Each customer has a unique Key Encryption Key (KEK) used to encrypt and protect a series of unique Data Encryption Keys (DEK). A unique DEK is created for each customer survey. A federal customer may request key destruction of the customer specific KEK which leads to survey data destruction. The data decommissioning procedures are established by the federal customer Brand administrator. | | | |

## Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

| | |
|---|---|
| | Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |
| X | Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. |
| | High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

| | | |
|---|---|---|
| X | Identifiability | Provide explanation:<br>PII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an |

| | | |
|---|---|---|
| | | individual. |
| X | Quantity of PII | Provide explanation:<br>The collection is for samples, therefore, a<br>serious or substantial number of individuals would be affected if there was loss, theft, or compromise of the data. |
| X | Data Field Sensitivity | Provide explanation:<br>The PII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm. |
| X | Context of Use | Provide explanation:<br>Disclosure of the PII may result in serious harm to the individual or organization. |
| X | Obligation to Protect Confidentiality | Provide explanation:<br>Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide requirements. Violations may result in serious civil or criminal penalties. |
| X | Access to and Location of PII | Provide explanation:<br>The PII is physically located on servers owned and managed by a third-party vendor at offsite facilities located in the United States. The third-party vendors used are Federal Risk and Authorization Management Program (FedRAMP) approved Cloud Service Providers (CSPs). |
| | Other: | Provide explanation: |

## Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

| |
|---|
| Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know. |

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

| | |
|---|---|
| | Yes, the conduct of this PIA results in required business process changes.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required business process changes. |

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

| | |
|---|---|
| | Yes, the conduct of this PIA results in required technology changes.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required technology changes. |