Privacy Threshold Analysis
for the
CEN29 Census Questionnaire Assistance (CQA)
U.S. Department of Commerce Privacy Threshold Analysis

CEN29 Census Questionnaire Assistance (CQA)

Unique Project Identifier: 006-000402200 00-07-01-02-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Census Questionnaire Assistance (CQA) Program at the U.S. Census Bureau (USCB), managed by General Dynamics Information Technology, Inc., interfaces with respondents over the phone to assist them with responding to and completing census questionnaires or other Frequently Asked Questions (FAQs) about the 2020 Census. CQA facilitates responses by fielding questions and, in some cases, by completing the interview with the respondent over the telephone.

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

CEN29/CQA is a major application implemented for the 2020 Decennial Census effort and provides contact center support on behalf of the USCB.

b) System location

The primary data center is located in Westminster, Colorado with a backup data center in Manassas, Virginia. The Program Management Office /Operational Command Center is located in the Washington DC area. The Contact Centers are numerous and will be located throughout the United States.

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

The CEN29/CQA system interconnects with both the CEN05/Enterprise Censuses and Surveys Enabling (ECaSE) platform for inbound and outbound operations and the CEN18/Census Data Lake (CDL) platform for reporting. In addition, CEN29/CQA interconnects with the
CEN05/ECaSE Internet Self Response (ISR) system and CEN05/Nonresponse Follow-up (NRFU) systems to provide interfaces for the CQA Customer Service Representative (CSR) to access the Census questionnaire forms online, while authenticating the CSR against the CQA identity and access management system.

d) The purpose that the system is designed to serve

The CQA program was established to aid in conducting the 2020 Decennial Census.

e) The way the system operates to achieve the purpose

The CQA Customer Service Representatives (CSR) agents provide real-time assistance to the members of the public (respondents) over the telephone. The assistance function involves providing the type of information and support that will increase the public’s participation in the Census, thereby improving the quality of the results and reducing costs. For the first time, the contact centers will serve as a primary response channel for the Decennial Census, the telephone channel will be actively promoted by the USCB as a data submission option, and CQA CSRs will actively request that respondents provide their Census data when they call.

This solution will enable the contact center to record the customer interactions across multiple sites and interactions, allowing the contact center to meet quality and regulatory compliance requirements. The recording solution provides reliable, high-quality recordings of both audio communications and desktop screen activity which will be provided to Census as required.

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

The caller provides their User ID (sent to them via USPS mail) that will allow the Customer Service Representative (CSR) to retrieve an address associated with that User ID, which the CSR then verifies with the caller prior to full data collection for that household. If the caller does not have a User ID, then the CSR will collect an address and questionnaire responses from the caller. Questionnaire responses can include gender, age, race/ethnicity, date of birth.

g) Identify individuals who have access to information on the system

Contractors and Government Employees

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

After a Customer Service Representative (CSR) authenticates a valid user with the Census Bureau system, the specific inbound or outbound data collection instrument will display and allow the CSR to collect information from the respondent over the phone. For inbound operations, no respondent data is retrieved. A caller can provide a User ID (sent to them via USPS mail) that will allow the CSR to retrieve an address associated with that User ID, which the CSR then verifies with the caller prior to full data collection for that household. If a caller does
not have a User ID, then the CSR will collect an address and the questionnaire responses from the caller.

For outbound operations, the Census Bureau provides the CSR a list of case IDs and phone numbers for households that require some type of phone follow-up. (These households had previously provided their census information.) Once a CSR is able to connect with someone over the phone during outbound operations, the case ID is required to proceed. After an eligible respondent is identified, the data collection instrument retrieves an address associated with that case ID which must be verified. Previously supplied household roster information is then reviewed with the respondent.

i) How information is transmitted to and from the system

A large outsourced Contact Center Operation (CCO) will support the CQA by executing inbound (respondent assistance) and outbound operations. The inbound operations will provide two main areas or tiers of assistance:

- Tier 1 – The Interactive Voice Response (IVR) system routes callers and provide answers to Frequently Asked Questions (FAQs) and other functions.

- Tier 2 – A Customer Service Representative (CSR) is the second tier of respondent support when IVR and web-based self-service tools have not been able to answer a respondent’s question. The CSRs will have the ability to capture respondent information into the ECaSE-Internet Self Response (ISR) system.

The outbound operations will provide support associated with maintaining and improving quality, such as verifying or completing respondent information for outbound telephone reinterview requests or coverage improvement interviews.
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.

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify): This PIA encompasses all the requirements for the Census 2020 system.</td>
</tr>
</tbody>
</table>

   — 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.

   —X— 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 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 nonetheless 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.

   —X— Yes. Please describe the activities which may raise privacy concerns.
   
   Audio Recordings

   — 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.552b)(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 about: (Check all that apply.)

____ Companies  
____ Other business entities  

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information  
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?  
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

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

____ DOC employees  
____ Contractors working on behalf of DOC  
__X__ 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 PII other than user ID?

__X__ 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.

4c. 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.

X 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, and/or 4c 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 the CEN29 CQA 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): Luis J. Cano
Signature of ISSO or SO: [Signature]
Date: 3/18/19

Name of Information Technology Security Officer (ITSO): Jeffery Jackson
Signature of ITSO: [Signature]
Date: 14 MAR 2019

Name of Technical Authorizing Official (AO): Kevin B. Smith
Signature of AO: [Signature]
Date: 3/14/19

Name of Business Authorizing Official (AO): Albert Fontenot
Signature of AO: [Signature]
Date: 3/14/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw
Signature of BPO: [Signature]
Date: 3/14/19