

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



**Privacy Threshold Analysis  
for the  
CEN29 Census Questionnaire Assistance (CQA)**

## U.S. Department of Commerce Privacy Threshold Analysis

### U.S. Census Bureau/ CEN29 Census Questionnaire Assistance (CQA)

**Unique Project Identifier:** [Number]

**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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 MAXIMUS Federal 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 answering 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 two CQA Cloud Service Provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) data centers are located in Highland Ranch, Colorado, and Sterling, Virginia with the CSP FedRAMP Security Operations Center and Network Operations Center located in Denver, Colorado. The CQA Program Management Office and the CQA Operational Command Center are located in Washington DC. During 2020 Census operations, CQA will utilize 10 contact centers located in Florida, Tennessee, Missouri, Arizona, Colorado, New York, Texas and South Carolina.

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 outbound operations and the CEN18/Census Data Lake (CDL) platform for inbound and outbound operations reporting. This connectivity is managed via the Service Oriented Architecture (SOA) Enterprise Service Bus (ESB). 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.

CEN29/CQA also interfaces with the following: the TTE Commercial datacenter to support Secure Development Life Cycle (SDLC) processes for code promotion purposes; the EPAY FedRAMP Cloud to provide access to timekeeping services to CQA operational staff, and; the Adobe Cloud to provide access to CQA operational staff access to training.

Additionally, CEN29/CQA interfaces with the following systems through Amazon Web Services based Application Programming Interfaces (API's) and file transfer utility:

- d) Oracle Talent Acquisition Cloud (OTAC) will be used to provision CQA accounts for these individuals to provide access to CQA applications and external cloud services such as EPAY/TKS and Adobe Connect.
- e) MAXIMUS Corporate SharePoint and CQA will both send and receive data necessary to CQA operations including daily briefings, standard operating procedures and knowledge articles.

*f) The purpose that the system is designed to serve*

Census Questionnaire Assistance (CQA) Program at the U.S. Census Bureau (USCB), managed by MAXIMUS Federal 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 answering questions and, in some cases, by completing the interview with the respondent over the telephone.

*g) The way the system operates to achieve the purpose*

The CQA program is part of the overall 2020 Decennial Census effort and provides contact center support on behalf of the USCB. The CQA has two primary functions:

- 1) Provide assistance for respondents by answering questions about specific items on the 2020 Census questionnaire form or other FAQs about the Census.
    - a. **Tier 1:** Provide telephone assistance through an automated Interactive Voice Response (IVR) system.
    - b. **Tier 2:** Provide real-time assistance by a CSR over the telephone.
  - 2) Provide an option for respondents to complete a 2020 Census interview over the telephone.
- 3) *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.

4) *Identify individuals who have access to information on the system*

Contractors and Government Employees

5) *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 an ID (sent to them via USPS mail) that will allow the CSR to retrieve an address associated with that ID. The CSR then verifies the address with the caller prior to full data collection for that household. If a caller does not have an ID, then the CSR will collect an address and the questionnaire responses from the caller.

For outbound operations, the Census Bureau provides the CQA contractor a list of case IDs and phone numbers for households that require some type of phone follow-up to confirm information. (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 or phone number of record 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 with the respondent. Previously supplied household roster information is then reviewed with the respondent.

6) *How information is transmitted to and from the system*

A large outsourced contact center operation will support CQA program by executing inbound (respondent assistance) and outbound operations. The inbound operations will provide two main tiers of assistance:

- Tier 1 – The automated IVR system routes callers and provides answers to FAQs.
- Tier 2 – A 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 answer questions and capture respondent information into the ECaSE- Internet Self Response (ISR) system.

The outbound operation will provide support associated with maintaining and improving quality, specifically verifying respondent information for coverage improvement interviews.

- Encrypted Multi-Protocol Label Switching (MPLS) is used to carry data and voice traffic between the call centers, network operation centers (NOC) /security operations centers (SOC)/Service Desk locations, and FedRAMP data centers
- Session Initiation Protocol (SIP) trunks to provide inbound/outbound call functions

Access to required Census-based applications will be facilitated from the FedRAMP data centers using firewalls, intrusion detection systems (IDS), URL filtering, traffic auditing, and logging functions All data traversing the FedRAMP boundary is encrypted and audited. This is implemented primarily through Secure Sockets Layer (SSL) for FedRAMP and web-based application services.

Data traversing to call centers, network security operation control centers, and for internal Census-based application or system interfaces will use IPsec/MPLS (Dynamic Multipoint Virtual Private Network [DMVPN]) to encrypt and secure traffic in transit. The delivery of recordings and transcription artifacts to the CEN18/CDL system is planned on a FIPS120-2 Level2 USB 3.0 compliant external storage media and will be delivered via approved courier provider FedEx to the USCB datacenter from CQA’s Sterling VA datacenter location. The delivery of these recording artifacts (as zip archives) is scheduled to commence at the end of operations as part of close-out activities. This USB-based transfer of non-production based recordings to the external storage media shall also be conducted additional prior to operations for purposes of performance and resiliency testing. In both cases, the activation of the port to use for the USB-based transfer method will be approved per USCB Risk Acceptance process initiated by the CQA Government Program Management Office (GPMO) team.

**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.*

| <b>Changes That Create New Privacy Risks (CTCNPR)</b>  |  |                        |                                    |
|--|--|------------------------|------------------------------------|
| 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 PIA includes the addition of CEN29 outbound operations which was included in phase 1b and services from multiple FedRAMP Cloud Service Providers included in Phase 2. |  |                        |                                    |

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   | X | 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.

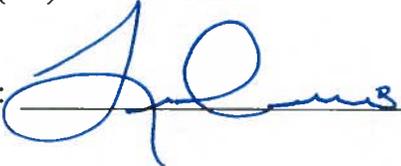
***If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.***

### CERTIFICATION

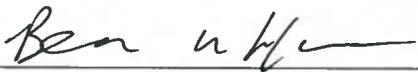
  X   I certify the criteria implied by one or more of the questions above **apply** to the CEN29 CQA and as a consequence of this applicability, I will perform and document a PIA for this IT system.

       I certify the criteria implied by the questions above **do not apply** to the [CEN29 CQA] 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:  Date: 9/19/2019

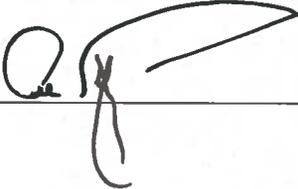
Name of Information Technology Security Officer (ITSO): Beau Houser

Signature of ITSO:  Date: 3 Oct 19

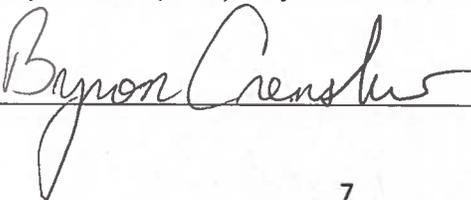
Name of Technical Authorizing Official (AO): Kevin B. Smith

Signature of AO:  Date: 10/15/19

Name of Business Authorizing Official (AO): Albert E. Fontenot Jr.

Signature of AO:  Date: 15 Oct 19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO:  Date: 10/31/19