

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



**Privacy Threshold Analysis
for the
CEN30 American Community Survey**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/CEN30 American Community Survey

Unique Project Identifier: 006-000400100

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).

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

The CEN30 IT system is considered a major application. The system maintains American Community Survey (ACS) data stored and processed in Statistical Analysis System (SAS) environments on Census Bureau servers.

b) System location

These servers are located in the Bowie Computer Center (BCC) and are accessed by workstations within the American Community Survey Office (ACSO) and other groups around the Census Bureau headquarters.

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

The system interconnects with the following systems:

- CEN05 - to support Stateside and Puerto Rico (PR) ACSO Housing Unit (HU) Data Collection, including the Remote Alaska (RA) operation and Group Quarters (GQ) Data Collection operations for stateside, PR, and RA, including Federal Prisons. This document does not cover the interfaces that support Re-interview (RI).
- CEN13 - to deliver the community survey data to CEN13 in order to integrate administrative records data
- CEN11 - to allow ACSO to transfer POP Estimates

- CEN06 - to support the American Community Survey (ACS) and Puerto Rico Community Survey (PRCS).

d) The purpose that the system is designed to serve

PII is collected from the public to produce national statistical information. The American Community Survey (ACS) is an ongoing survey that provides data every year -- giving communities the current information they need to plan investments and services. Information from the survey generates data that help determine how more than \$400 billion in federal and state funds are distributed each year.

e) The way the system operates to achieve the purpose

The ACS questionnaires and survey instruments are used to collect data from the Housing Unit (HU) population. Some of the information collected by the components in the CEN30 IT system are: name, address, age, sex, race, family and relationships, income and benefits, health insurance, education, veteran status, disabilities, where you work and how you get there, where you live and how much you pay for some essentials and food stamp benefits.

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

Some of the information collected by the components in the CEN30 IT system are: name, address, age, sex, race, family and relationships, income and benefits, health insurance, education, veteran status, disabilities, where you work and how you get there, where you live and how much you pay for some essentials and food stamp benefits.

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

The user community consists of sworn federal and contracted employees of the Bureau of the Census.

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

The ACSO staff use statistical software to refine the data, then make edited datasets available to users within the Census Bureau. Only employees assigned to ACSO will have access to this data.

Records that contain PII such as name and address are kept in separate files and are only used minimally for data collection processing. A non-PII ID is generated as a key to retrieve records on the production data files.

Once the questionnaires are received, they undergo a data preparation process. The broad purpose of data preparation and processing is to take the response data gathered from each survey collection and format it in a way that it can be used to produce survey estimates.

Files that need editing, known as edit input files, are created during the data preparation phase by merging operational status information for each Housing Unit and Group Quarters facility with the files that include the survey response data. The combined data must go through a number of processing steps before they are ready to be tabulated. Once the edit input files are prepared, the edit and imputation process is initiated. Editing and imputation ensure that the final data are consistent and complete. Subject matter analysts thoroughly examine and approve the results of the edit and imputation process.

i) How information is transmitted to and from the system

Data is collected by internet, mail, telephone, and in person. Data collection instruments are used for all four of these modes of data collection.

- The internet instrument is a web-based system where respondents use a respondent ID to access and complete the questionnaire.
- Mail questionnaires are received, processed in batch, and sent to the data capture unit in the Census Bureau's National Processing Center (NPC).
- The telephone instrument is a computer-assisted telephone interview (CATI) instrument that utilizes computers for data collection.
- The personal interview instrument is a computer-assisted personal interview (CAPI) instrument that utilizes in-person interviewers that conduct interviews for data collection on the computer.

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 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.

CEN30 ACSO PTA CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to CEN30 ACSO 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): Barbara M. LoPresti

Signature of SO: Barbara LoPresti Digitally signed by Barbara LoPresti Date: 2020.07.21 12:05:01 -04'00' Date: _____

Name of Chief Information Security Officer: Beau Houser

Signature of CISO: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2020.08.05 23:32:48 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.08.20 10:42:27 -04'00' Date: _____

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

Signature of AO: Albert E Fontenot Digitally signed by Albert E Fontenot Date: 2020.08.19 09:28:58 -04'00' Date: _____

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO: KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2020.08.06 12:37:26 -04'00' Date: _____

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.08.20 10:42:55 -04'00' Date: _____