

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



**Privacy Threshold Analysis
for the
CEN13 Center for Enterprise Dissemination (CED)**

U.S. Department of Commerce Privacy Threshold Analysis

Bureau of the Census, CEN13 Center for Enterprise Dissemination (CED)

Unique Project Identifier: 006-000400700

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

CEN13 is a general support system.

b) System location

Bowie, Maryland

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

CEN13 interconnects with the following Census Bureau systems:

- ADEP ITO: Associate Directorate for Economic Programs (CEN36)
- EAD: Economic Census and Surveys and Special Processing (CEN03)
- GEO: Geography (CEN07)
- DSD: Demographic Census, Surveys and Special Processing (CEN11)
- CAES: Concurrent Analysis and Estimation System (CEN18)
- PEARSIS: Production Environment for Administrative Record Staging, Integration and Storage (CEN08)
- DMS: Data Management System (CEN18)
- ACSO: American Community Survey (CEN30)
- ITMD: Foreign Trade Division Applications (CEN34)
- DSCMO-DSSD: Decennial (CEN08)

- UTS: Unified Tracking System (CEN05)
- IDMS: Identification Management System (CEN01)
- ERD: Economic Reimbursable Surveys Division (CEN03)

d) The purpose that the system is designed to serve

Administration and research is the mission of the CEN13 program for statistical purposes:

For administrative matters:

The PII/BII is used for record linkage. SSNs are used to assign protected identification keys (PIKs) after which SSN and other PII are dropped from the file. After the PIK is assigned files are linked only by PIK. In some cases, PII is used for linkage activities instead of a PIK when the production or research need necessitate use of PII. The use of PII for linkage activities requires senior management approval.

Research, Improvement/support of Census Bureau programs through use of administrative and other non-survey data, Quality assurance, and statistical purposes:

Record linkage using BII and PIKs facilitates research to improve and support existing Census Bureau programs and creation of beta data products. These products use innovative techniques that leverage existing data and reduce the burden on respondents.

e) The way the system operates to achieve the purpose

CEN13 provides a research platform with high performance computing and standard statistical tools to conduct research to improvement/support of Census Bureau Programs through use of administrative and other non-survey data, quality assurance, and statistical purposes. The research platform interacts with the Data Management System (DMS), the Identification Management System (IDMS) and the Center for Enterprise Dissemination Management System (CMS) to make sure the research projects are approved and creates project space for the project on the research platform. The system provides access to project space only for the users that have been approved to work on the project. The project has access only to the data that has received prior approval to use. Researchers execute their computational model on the research platform and write the outputs into their project space.

For internal Census staff users, the Data Management System (DMS) is used to perform management and tracking functions for research proposal and active projects. The DMS is used to track the status and activity of all projects from initial conception through completion and close out.

For external Federal Statistical Research Data Center (FSRDC) users, the CED Management System (CMS) is used to perform management and tracking functions for research proposals and active projects. The CMS is used to track the status and activity of all projects from initial conception through completion and close out. Data is available only to researchers who have received prior approval.

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

The CEN13 Center for Enterprise Dissemination IT System includes data maintained by the Census Bureau's Associate Director for Research and Methodology (ADRM). The CEN13 IT system covers the personally identifiable information (PII) and Business identifiable information (BII) from each of the research centers maintained by the system. The ADRM data holdings include census and survey data including personally identifiable information (PII) and business identifiable information (BII) received from other Census Bureau IT systems identified in item c below, administrative records from other federal, state, and local agencies, and proprietary data files from commercial vendors and some non-profit organizations. The Census Bureau is required by law to obtain and reuse data that already exists at other agencies to reduce the burden on people who respond to census and survey questions. By reusing data that already exists elsewhere, and linking it to census and survey data, Census is able to conduct research that provides a more holistic view of the people present in, and the economy of, the United States. Information received from administrative records are protected from unauthorized disclosure under Title 13 U.S.C. The data in this IT system is used for statistical purposes and for research and operations to improve record linkage methods for surveys, including the decennial census.

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

Government employees, contractors, and Special Sworn Status employees of the Census Bureau

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

The data files are stored on disk in various formats determined by the statistical software that they are to be processed with (SAS, Stata, R, etc.). Users use these statistical software packages to analyze the data. Data may also be stored in relational databases and retrieved through database queries. Retrieval of the data is performed only by authorized Census Bureau staff who have a need to know and are authorized through DMS. Data records may be retrieved using, PII, BII, protected identification key (PIK), Social Security Number (SSN) or other field defined within the system depending on the application or model.

i) How information is transmitted to and from the system

Data is transmitted by Secure File Transfer Protocol (SFTP) and Linux based tool to synchronize files between systems.

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): Citizenship information obtained from administrative records.			

- 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): Matching citizenship information from administrative records to Census files.			

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.

<p>Provide an explanation for the business need requiring the collection of SSNs, including truncated form. SSNs are often included in administrative records datasets acquired in support of the Census Bureau's Title 13 authority to collect these data. When SSNs are present in these data they serve as one of several components used in a matching or look-up process to assign an anonymized protected identification key (PIK) to the record.</p>
<p>Provide the legal authority which permits the collection of SSNs, including truncated form. The authority to obtain the SSN via admin records under 13 USC Section 6.</p>

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 CEN13 Center for Enterprise Dissemination (CED) 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): Robert Sienkiewicz

Signature of SO: ROBERT SIENKIEWICZ Digitally signed by ROBERT SIENKIEWICZ Date: 2020.06.04 17:08:08 -04'00' Date: _____

Name of Chief Information Security Officer: Beau Houser

Signature of ITSO: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2020.07.02 09:39:52 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.06.22 15:50:10 -04'00' Date: _____

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO: KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2020.07.21 14:28:04 -04'00' Date: _____

Name of Business 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: 2020.06.04 17:12:02 -04'00' Date: _____

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.06.22 15:50:32 -04'00' Date: _____