U.S. Department of Commerce
Bureau of the Census

Privacy Threshold Analysis
for the
CEN13 Center for Economic Studies
U.S. Department of Commerce Privacy Threshold Analysis

Bureau of the Census/Center for Economic Studies (CEN13)

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 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).

a) Whether it is a general support system, major application, or other type of system
   The CEN13 Center for Economic Studies (CES) IT system is classified as other. The CEN13 CES IT system includes data maintained by the Research and Methodology Directorate and the Census Bureau. The CES CEN13 IT system consists of the CED Management System (CMS), MySQL (Database), NX Server, the Integrated Research Environment (IRE), and SAS Foundation.

b) System location
   CEN13 CES is housed at the Bowie Data Center (BCC).

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
   CEN13 CES IT interconnects with other Census Systems including
   - ADEP ITO Associate Directorate for Economic Programs (CEN36)
   - EAD Economic Census and Survey and Special Processing (CEN03)
   - GEO Geography (CEN07)
   - DSD Demographic Census, Surveys and Special Processing (CEN03)
   - 2020 Census (CEN08)

d) The purpose that the system is designed to serve
   CEN13 IT is designed to serve as a tool for administrative matters (e.g., External Federal Statistical Research Data Center (FSRDC) project tracking) and research projects in support of Census Bureau programs.
e) The way the system operates to achieve the purpose

For Internal Census projects, the Data Management System (DMS) is used to perform management and tracking functions for research proposals and active projects. The DMS is used to track the status and activity for all projects from start through completion and close out. For External Federal Statistical Research Data Center (FSRDC) projects, the CED Management System (CMS) is used to track the status and activity of all projects from initiation through completion and close out. The information on data and users approved for projects in the DMS and CMS defines access controls on CEN 13 systems.

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

The CEN13 IT system covers the personally identifiable information (PII) and business identifiable information (BII) maintained within the system. The CEN13 data holdings include census and survey data which may contain name, gender, age, date of birth etc. from across the Census Bureau, administrative records from other federal agencies and proprietary data files from commercial vendors and some non-profits.

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

Internal Census staff users and contractors and Special Sworn Status (SSS) individuals have access to information on the system. This is documented in the Census Bureau’s Data Management System (DMS).

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

For internal Census projects, the DMS is used to perform management and tracking functions. The DMS is used to track the status and activity of all projects from initial conception through completion and close out. For external FSRDC users the CED Management System (CMS) is used to perform management and tracking functions. The CMS is used to track the status and activity of all projects from initial conception through completion and close out.

i) How information is transmitted to and from the system

The CEN13 IT System uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) Special Publication 800 series. These security controls include but are not limited to the mandatory use of HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution.
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                      |
     | b. Anonymous to Non-Anonymous                 | e. New Public Access                        |
     | c. Significant System Management Changes      | f. Commercial Sources                       |
     | 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.*

   ____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 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. *Please describe the activities which may raise privacy concerns.*

   ____ 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.)."
1. Yes, the IT system collects, maintains, or disseminates BII about: (Check all that apply.)

   ___ Companies
   ___ Other business entities

   ___ 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...."

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

       ___ DOC employees
       ___ Contractors working on behalf of DOC
       ___ 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?

   ___ 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.

___ 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 CEN13 CES 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): Lucia Foster

Signature SO: ___________________________ Date: 4/25/19

Name of Information Technology Security Officer (ITSO)/Chief Information Officer (CIO): Jeffery W. Jackson

Signature of ITSO/ CIO: ___________________________ Date: 4/26/19

Name of Authorizing Official (AO): Kevin Smith, John Eltinge

Signatures of AO’s: ___________________________ Date: 6/24/19

Name of Bureau Chief Privacy Officer (BCPO): Byron Crenshaw

Signature of BCPO: ___________________________ Date: 8/15/19