Version Number: 01-2019

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

Privacy Threshold Analysis
for the
CEN11 Demographic Census, Surveys, and Special Processing

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/ CEN11 Demographic Census, Surveys, and Special Processing

Unique Project Identifier: 006-000400500

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 U.S. Census Bureau's CEN11 Demographic Census, Surveys, and Special Processing System is an IT system comprised of a collection of major and minor applications that support the Demographic Directorate business functions.

(b) System location

All CEN11 components reside on servers located within the Census Bureau's Bowie Computer Center (BCC).

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

CEN11 applications interconnect with internal Census Bureau IT systems to leverage enterprise services (CEN01 Data Communications, CEN16 Network Services), inherit security controls provided by the Enterprise Common Control Providers (ECCP), and transmit/receive data required for statistical data collection and processing to/from these IT systems: CEN03 Economic Census and Surveys and Special Processing, CEN13 Center for Enterprise Dissemination (CED), CEN18 Enterprise Applications, CEN30 American Community Survey Office, CEN05 Field Systems Major Application System, and CEN15

Centurion. CEN11 also interconnects with external IT systems for the purpose of statistical data collection and processing. Each external interconnection has a different function and purpose as described below:

The interconnection between CEN11 and the Bureau of Labor Statistics (BLS) is used to transmit data between Census Bureau Special Sworn Status (SSS) individuals located at BLS and BLS agents located at the Census Bureau in support of the Current Population Survey, the Consumer Expenditure Survey, and the American Time Use Survey.

The interconnection between CEN11 and the National Center for Health Statistics (NCHS) is used to make data available from Census Bureau resources to return processed data to NCHS (using the CDC Secure Access Management System).

(d) The purpose that the system is designed to serve

Personally identifiable information (PII) is collected through various demographic data surveys, IT systems, and programs to produce national statistical information.

The data is used to calculate and process the statistical data input for the purpose of creating statistical information and reports (i.e. Annual household and group quarters' population estimates by age, sex, race, and origin for counties).

(e) The way the system operates to achieve the purpose

The survey data for demographic programs is collected using a multi-mode approach made up of:

- Face-to-face Interviews conducted by Field Representatives (FRs) using Computer Assisted Personal Interview (CAPI) on CEN05 Field IT systems;
- Telephone Interviews conducted by centralized interviewers using Computer Assisted Telephone Interview (CATI) (CEN05 Field) or by FRs conducting decentralized telephone interviews using CAPI;
- Web-based interviews by respondents. Respondents use a web-based application instrument that resides on the Census Bureau network via CEN15 Centurion. Respondents use their personal computers to access Centurion.

Once the information is collected by the survey instruments, the information is stored in a CEN11 repository for use.

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

PII is collected from the public through various demographic data surveys, programs, focus groups/cognitive interviews, or methodological studies to produce national statistical information. The data is used to calculate and process the statistical data input for the purpose of creating statistical information and reports (e.g., Annual household and group quarters' population estimates by age, sex, race, and origin for counties, etc.).

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

U.S. Census Bureau employees and contractors

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

Files are identified with either a Case ID or control number, or by a personal identifier (e.g. Social Security Number (SSN)) for certain surveys or special research projects. The specified Case ID, control number, or personal identifier is used to retrieve the individual case within a file.

(i) How information is transmitted to and from the system

The information is collected/transmitted using FIPS 140-2 compliant encryption.

(j) Any information sharing conducted by the system

There is PII being shared as follows:

- The Census Bureau provides access to staff at Department of Housing and Urban Development (HUD) with Special Sworn Status (SSS) for the American Housing Survey (AHS) via the Census Bureau Virtual Desktop Infrastructure (VDI) in their Survey Sponsor Data Center. The same is true of the U.S. Department of Health and Human Services Health Resources and Services Administration (HRSA) and HRSA's Maternal and Child Health Bureau (MCHB) for the National Survey of Children's Health (NSCH) and the U.S. Department of Health and Human Services and HRSA's National Center for Health Workforce Analysis for the National Sample Survey of Registered Nurses (NSSRN).
- The Census Bureau provides some Bureau of Labor Statistics (BLS) Staff access to Current Population Survey (CPS), American Time Use Survey (ATUS), and Consumer Expenditure Survey (CES) data on a CEN11 Server. BLS Staff have Special Sworn Status (SSS) to have Census Bureau accounts to access the server. Consumer Expenditure staff at BLS access CPS data for weighting purposes.
- The Census Bureau sends data files to the National Center for Health Statistics (NCHS) for the National Ambulatory Medical Care Survey (NAMCS), the National Hospital Ambulatory Medical Care Survey (N(H)AMCS) and National Health Interview Survey (NHIS). Data transfers are conducted through the Centers for Disease Control and Prevention (CDC) Secure Access Management Services (SAMS).
- The Census Bureau sends data files to the National Center for Education Statistics (NCES) for the National Household Education Survey (NHES), the School Survey on

Crime and Safety (SSOCS), the Schools and Staffing Survey (SSS), the Private School Survey (PSS), the National Teacher and Principal Survey (NTPS), the Teacher Follow-up Survey (TFS), the Principal Follow-Up Survey (PFS) and the Beginning Teacher Longitudinal Survey (BTLS). Data transfers are conducted through the Institute of Education Sciences (IES) Members Site.

- The Census Bureau provides restricted access to staff of the National Center for Science and Engineering Statistics (NCSES) at the National Science Foundation (NSF). Staff with access have Special Sworn Status and connect via the Census Bureau VDI.

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.*

_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). *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.

__X_ 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.

_X_ 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."

_X_ 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
_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 Social Security numbers (SSNs), including truncated form?

_X_ 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. The justification for the necessity of collecting this information, taken from the latest approved OMB ICR supporting statement is below: Social Security Number and Health Insurance Claim Number: The last four digits of the Social Security Number (SSN) is asked on the NHIS questionnaire to allow linkage with administrative and vital records, such as the National Death Index (NDI). The NDI is a computerized central file of death record information. It is compiled from data obtained by NCHS from the State vital statistics offices. The data contain a standard set of identi-fying information on decedents from 1979 to the present. Records are matched using Social Security

Number and other variables such as name, father's surname, date of birth, sex, state of residence, and marital status. Of these, Social Security Number is the most important identifier for successful matching. The last four digits has been shown to be nearly as effective for matching as the full number.

The Social Security Number is also used by the Medical Expenditure Panel Study to help track the location of respondents who have changed residence since their NHIS interview. Finding a correct address for respondents is essential to maintaining response levels at an acceptable level in linked surveys, and the Social Security Number is a key item for establishing a correct address.

Medicare beneficiaries are given a health insurance claim (HIC) number that is their (or their spouse's) SSN with an alphabetic prefix. The NHIS also asks for the last four digits of that number so that the NHIS data can be linked to Medicare claims information for purposes of statistical research.

____ 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?

_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.

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.

_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, 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 FOR CEN11

_X__ I certify the criteria implied by one or more of the questions above **apply** to CEN11 Demographic Census, Surveys, and Special Processing 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): Jeffrey Sisson

Signature of SO: JEFFREY SISSON Digitally signed by JEFFREY SISSON Date: 2020.09.01 10:21:24 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Beau Houser

Signature of CISO: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2020.09.08 10:03:58 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.09.21 11:27:41 -04'00' Date: _____

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO: KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2020.09.10 12:09:35 -04'00' Date: _____

Name of Business Authorizing Official (AO): Victoria Velkoff

Signature of AO: VICTORIA VELKOFF Digitally signed by VICTORIA VELKOFF Date: 2020.09.10 10:31:53 -04'00' Date: _____

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BCO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.09.21 11:28:08 -04'00' Date: _____