Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Associate Directorate for Demographic Programs (DEMO)
Demographic Census, Surveys, and Special Processing

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau / DEMO 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 Demographic Programs Directorate (DEMO) 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 DEMO 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)

DEMO applications interconnect with internal Census Bureau IT systems to leverage enterprise services provided by the following divisions:

- Data Communications system
- Network Services system

DEMO applications inherit security controls provided by the Enterprise Common Control Providers (ECCP):

- Data Communications system
- Network Services system

In addition, DEMO transmits/receives data required for statistical data collection and processing to/from these IT systems:

- Economic Census and Surveys and Special Processing
- Center for Enterprise Dissemination (CED)
- Enterprise Applications
- American Community Survey Office
- Field Systems Major Application System
- Centurion
- Geography
- Decennial
- Longitudinal Employer-Household Dynamics (LEHD)
- American Fact Finder – Data Access & Dissemination Systems (AFF-DADS)
- Economic Applications Division (EAD) Windows Applications System

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

Utilizing virtual desktop infrastructure (VDI), Census Bureau provides Department of Housing and Urban Development (HUD) staff with Special Sworn Status (SSS) access to the American Housing Survey (AHS) and other surveys they sponsor.

The same is true for U.S. Department of Health and Human Services (HHS) Health Resources and Services Administration (HRSA), HRSA's Maternal and Child Health Bureau (MCHB), HRSA's National Center for Health Workforce Analysis (NCHWA), the New York City Department of Housing Preservation and Development (HPD), and the staff of the National Center for Science and Engineering Statistics (NCSES) at the National Science Foundation (NSF). These entities gain access to these data utilizing VDI.

The interconnection between DEMO 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 Centers for Disease Control and Prevention (CDC) Secure Access Management System (SAMS)).

(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 (FR) using Computer Assisted Personal Interview (CAPI) on Field IT systems;
- Telephone interviews conducted by centralized interviewers using Computer Assisted Telephone Interview (CATI) (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 Centurion. Respondents use their personal computers to access Centurion.

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

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

PII is collected from the public through various demographic surveys, programs, focus groups/cognitive interviews, IT systems 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.)

(e) 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., last four of the 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 Federal Information Processing Standards (FIPS) 140-2 compliant encryption.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

_x___ 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): Current Population Survey (CPS) Annual Social and Economic Supplement (ASEC) collects federal stimulus payments, and federal tax credits as part of their measurement of how much income a person earned in a year and what government programs they use. National Crime Victimization Survey (NCVS) asks socio-demographic questions, including sexual orientation and gender identity, to allow researchers and policy makers to better understand the relationships between these variables and experiences with criminal victimization. SIPP collects federal tax stimulus payments and federal tax credits so that economic well-being and income can be calculated.					

____ 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 or 01-2017). *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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

___ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

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.)*

_X__ DOC employees
____ 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. SSSN and Health Insurance Claim Number (HCN): The last four digits of the SSN is asked on the National Health Interview Survey (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 contains a standard set of identifying information on decedents from 1979 to present. Records are matched using SSN and other variables such as name, father's surname, date of birth, sex, state of residence, and marital

status. Of these, SSN is the most important identifier for successful matching. The last four digits have been shown to be nearly as effective for matching as the full number. The SSN is also used by the Medical Expenditure Panel Study to help track the location of respondents who have changed residence since their NHIS interview. Findings a correct address for respondents is essential to maintaining response levels at an acceptable level in linked surveys, and the SSN 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.
Provide the legal authority which permits the collection of SSNs, including truncated form. 13 U.S.C. Section 8(b); 42 U.S.C. Section 242k; and 42 U.S.C. 299a

____ 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 SAOP 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 Demographic Programs Directorate (DEMO) 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 DEMO Demographic Census, Surveys, and Special Processing and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Jeffrey Sisson Office: Chief, Demographic Surveys Division (DSD) Phone: (301) 763-2082 Email: jeffrey.d.sisson@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: JEFFREY SISSON Digitally signed by JEFFREY SISSON Date: 2021.12.20 16:29:25 -05'00' Date signed: _____	**Chief Information Security Officer** Name: Beau Houser Office: Chief, Office of Information Security Phone: (301) 763-1235 Email: beau.houser@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2022.01.05 10:57:10 -05'00' Date signed: _____
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763-7997 Email: byron.crenshaw@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.01.10 16:42:16 -05'00' Date signed: _____	**Agency Authorizing Official** Name: Luis Cano Office: Chief Information Office Phone: (301) 763-3968 Email: luis.j.cano@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2022.01.06 14:09:10 -05'00' Date signed: _____
Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763-7997 Email: byron.crenshaw@census.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.01.10 16:42:40 -05'00' Date signed: _____	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.