Version Number: 01-2015

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

Privacy Impact Assessment
for the
CEN11 Demographic Census, Surveys, and Special Processing

Reviewed by: Byron Crenshaw, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2019.08.20 18:08:21 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/Demographic Census, Surveys, and Special Processing

Unique Project Identifier: 006-000400500

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system

The U.S. Census Bureau's CEN11 Demographic Census, Surveys, and Special Processing System is a system comprised of components that support the Demographic Directorate business functions. The component within CEN11 that contains PII is a Commercial off the Shelf (COTS) product used by Census Bureau demographic programs for data access, transformation, reporting, and statistical analysis. Some of the demographic data maintained in this system are Name, date of birth, telephone number, occupation, military service information (if applicable), medical information, financial information etc.

(b) a description of a typical transaction conducted on the system

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

- Face-to-face or telephone induction interviews
- Field Representatives (FR)
- Web-based respondents

The information is collected by using:

Web-based 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.

Introduction interviews are collected using electronic instruments – Computer-Assisted Personal Interviewing (CAPI) (a CEN05 component).

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

(c) 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).

- The Census Bureau provides some Bureau of Labor Statistics (BLS) Staff access to Current Population Survey (CPS) and Consumer Expenditure Survey (CES) data on a CEN11 Server in the DMZ. BLS Staff have Special Sworn Status (SSS) to have Census accounts to access the server. Consumer Expenditure staff at BLS access CPS data for weighting purposes.
- Census Bureau sends a file containing respondent addresses to BLS for the Telephone Point of Purchase Survey (TPOPS).
- 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.

(d) a citation of the legal authority to collect PII and/or BII

13 USC sections 8(b), 182 and 18 U.S.C. 2510-2521

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

This is categorized as a moderate system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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):					

__x_ This is an existing information system without changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	x	e. File/Case ID		i. Credit Card	
b. Taxpayer ID	x	f. Driver's License		j. Financial Account	
c. Employer ID	x	g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: The last 4-digits of the SSN is used in admin records matching to the National Health Interview Survey (NHIS).

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 resi-dence, 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.

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name	x	h. Place of Birth	x	n. Financial Information	x
c. Alias	x	i. Home Address	x	o. Medical Information	x
d. Gender	x	j. Telephone Number	x	p. Military Service	x
e. Age	x	k. Email Address	x	q. Physical Characteristics	x
f. Race/Ethnicity	x	l. Education	x	r. Mother's Maiden Name	
s. Other general personal data (specify): Citizenship					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	x
c. Voice Recording/Signatures	x	f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	x
Telephone	x	Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal	x	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	x
Third Party Website or Application			x		
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	x	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): For Computer Assisted Personal Interviewing (CAPI), the Demographic Programs Directorate (DEMO) uses Computer-audio recording interviewing (CARI) for select interviews for the Survey of Income and Program Participation (SIPP); future plans are to incorporate CARI for all demographic CAPI surveys. For Computer Assisted Telephone Interviewing (CATI) surveys, the NICE Sentinel 2.5 system is used to record selected interviews for Quality Assurance (QA) purposes. Both types of recordings contain PII.			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For statistical purposes (i.e., Censuses/Surveys)			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII is used to process numerous national statistical surveys and other demographic data programs.

The data is used to calculate, process, and manipulate 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).

The information that is collected in this system is from members of the public.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x	x	x

DOC bureaus			
Federal agencies		x	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

x	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: CEN11 shares information with CEN03, CEN07, CEN08, CEN13, CEN14, CEN18, CEN19, and CEN30. CEN11 receives information from CEN13, CEN30, and CEN35. The CEN11 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 use of mandatory 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 as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors	x		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _ https://www.census.gov/about/policies/privacy/privacy-policy.html_____.	
x	Yes, notice is provided by other means.	Specify how: Official correspondence letter or email from the Census Bureau to respondents.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: CEN11 surveys are voluntary. Individuals may refuse to participate in the survey or, if they do participate, they may refuse to answer specific questions.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
x	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For records covered under SORNs Census -3 and SORN Census-7 the data is collected for statistical purposes and there is no opportunity to consent to uses of the data.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
x	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For records covered under SORNs Census -3 and SORN Census-7 there are no access to the records since the data is collected for statistical purposes.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control *AU-03, Content of Audit records*.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ____7/12/2018____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): Publications are approved by the Disclosure Reviewed Board.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. Census also deploys a DLP solution as well.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*:
x	Yes, a SORN has been submitted to the Department for approval on (date). 1. Census -3, Demographic Survey Collection (Census Bureau Sampling Frame) submitted on 7/22/16. 2. Census-7, Demographic Survey Collection (non-Census Bureau Sampling Frame) submitted on 7/22/16.
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: N1-29-99-5, N1-29-89-3, N1-29-87-3, N1-29-86-3, NC1-29-85-1, NC1-29-79-7, and GRS 3.1 GRS 3.2 GRS 4.1, GRS 4.3
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing		Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII/BII collected can be directly used to identify individuals
X	Quantity of PII	Provide explanation: The collection is for Census Bureau Censuses and surveys, therefore, a severe or catastrophic number of individuals would be affected if there was loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII/BII, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the act of collecting and using the PII/BII in this IT system or the PII/BII itself may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with organization or mission- specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government- wide or industry-specific requirements. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	PII/BII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access is limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals. Access is only allowed by organization-owned equipment outside of the physical locations, and only with a secured connection.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

x	Yes, the conduct of this PIA results in required business process changes. Explanation: Next PTA will be update selection in question 2 to yes to address audio recordings and consistency with section 3.1 of the PIA.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.