

EXHIBIT A

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



Privacy Impact Assessment
for the
CEN08 Decennial Information Technology Division (DITD)

Reviewed by: , 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

Dr. Catrina D. Purvis

LISA MARTIN

Digitally signed by LISA MARTIN
DN: c=US, o=U.S. Government, ou=Department of
Commerce, ou=Office of the Secretary, cn=LISA MARTIN,
0.9.2342.19200300.100.1.1=13001000105292
Date: 2018.06.26 14:23:47 -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/CEN08 DITD

Unique Project Identifier: 006-000400400

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

CEN08 Decennial manages the development and implementation of major decennial census applications utilized by the Decennial Census Program. These applications process response data from census tests and 2020 Census operations, and perform quality assurance mechanisms for various census operations. These applications also facilitate the acquisition of software and integration services required to support the U.S. Census Bureau during the preparation and actual Decennial Census operations.

Some examples of the information collected, maintained, and/or disseminated within CEN08 Decennial are names, addresses, gender, age, date of birth, race, email, education, telephone number and salary.

The CEN08 Decennial IT system monitors the cost, schedule, and technical performance milestones for each software system or application utilized for decennial census purposes. The CEN08 IT system manages the development and implementation of software and systems necessary to support collection, processing, and tabulation of census data.

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

The CEN08 Decennial IT system provides updates and unit (e.g., a home, a building, or miscellaneous structure) status information to various divisions within the Census Bureau that maintain address information (e.g., street addresses, and status and control information for households and other living quarters).

In addition, CEN08 applications confirm receipt of response data. They also provide validation and acknowledgment of the data received from various IT systems.

(c) any information sharing conducted by the system

The CEN08 Decennial IT system shares information internally within the Census Bureau (to CEN07 and CEN11).

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

Title 13, U.S.C. Section 6c
 Title 13, U.S.C. Section 141
 Title 13, U.S.C. Section 193
 Title 26, U.S.C. 6103(j)

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

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is Moderate.

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):					

☒ 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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID	X	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:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	

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

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		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	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify): Audit Logs					

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			
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	X
Third Party Website or Application					
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		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	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).

The PII that is collected, maintained, or disseminated will be used for:

Statistical Purposes (i.e. Censuses/Surveys):

The U.S. Census Bureau collects, maintains, and disseminates PII data to produce national statistical information from the U.S. population. This information determines the distribution of Congressional seats to states, aids in the decisions about what community services to provide, determines the amount distributed of more than \$400 billion in federal funds to local, state and tribal governments each year.

The PII collected, maintained, and/or disseminated by the CEN08 IT system is in reference to 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		
DOC bureaus			
Federal agencies			
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:
---	---

	<p>CEN08 shares information with IT systems within the Census Bureau (i.e. CEN07 and CEN11). CEN08 receives information from a number of other IT systems within the Census Bureau (i.e. CEN05 and CEN07).</p> <p>CEN08 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.</p>
	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: http://www.census.gov/about/policies/privacy/privacy-policy.html
	Yes, notice is provided by other means. Specify how:
	No, notice is not provided. Specify why not:

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

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: According to Title 13, Section 221 (Census, Refusal or neglect to answer questions; false answers) of the United States Code, persons who fail or refuse to respond to the mail-back census form, or refuse to respond to a follow-up Census Bureau taker can be fined up to \$100. Persons who knowingly provide false information to the Census Bureau can be fined up to \$500.

		For Census Bureau employees who access systems in CEN08 providing PII is a requirement for employment.
--	--	--

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 by SORN Census-5, Decennial Census Programs, there are no access and consent requirements since the data is collected for statistical purposes only. For Census Bureau employees consent to particular uses of PII is a requirement for employment.

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 by SORN Census-5, Decennial Census Programs, there is no opportunity to review/update data unless the Census Bureau contacts the respondent for an update on their information. For Census Employees, employees have access to PII via the appropriate Human Resources applications that reside outside of the CEN08 IT system.

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 within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition to IT system processes that handle PII, all manual extractions for PII 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): <u>July 25, 2017</u> <input type="checkbox"/> 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.
	Other (specify):

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 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 Bureau that contains, transmits, or processes 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. The Census Bureau 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (list all that apply): Census-5 Decennial Census Program
	Yes, a SORN has been submitted to the Department for approval on (date).
	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: NI-29-05-01, NI-29-10-5, GRS 3.1, 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	X	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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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 collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
X	Quantity of PII	Provide explanation: The collection is for the decennial census, therefore, a serious or substantial number of individuals would be affected if there was loss, theft or compromise of the data. Serious collective harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: The PII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
X	Context of Use	Provide explanation: Disclosure of the act of collecting and using the PII in this IT system or the PII itself may result in serious harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII collected is required to be protected in accordance with 13 U.S.C .6c,141,193 and 26 U.S.C 6103 (j).
X	Access to and Location of PII	The PII is located on computers (including laptops) and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know including the Census Bureau regional offices and survey program offices, etc. Access is allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities.
	Other:	Provide explanation:

Section 12: Analysis

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	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.