

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



**Privacy Impact Assessment
for the
CEN07 Geography**

Reviewed by: Byron Crossman 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

for Dr. Catrina D. Purvis [Signature] 08/05/2019
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment CEN07 Geography

Unique Project Identifier: 006-000400900

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

CEN07 Geography consists of a number of applications that process geospatial and address data used for generating address frame for Census Bureau censuses and surveys. The information collected, maintained, and/or disseminated within CEN07 are addresses (personal and place of work), geocodes, attributes and descriptions of structures and Global Positioning System (GPS) coordinates. The applications in CEN07 generate maps that assist in performing the following functions:

- Boundary collection and validation;
- Address List Reviews;
- Field data collection operations; and the
- The Data product dissemination program, (map and geographic entity (county, city, block etc.) is made available for public use).

These applications also assist in facilitating geographic visuals for:

- assigning the residential housing units in each Census and sample survey to a specific geographic location (geocodes and GPS coordinates);
- developing a source file from which the U.S. Census Bureau can generate geographic tables. An example of a geographic table could be described as a table that lists all of the counties in a state, then all of the cities, tracts, or blocks within each county;
- creating summary cartographic products maps for data tabulation and customer support purposes. A summary cartographic products map is a map that displays codes for geography entities such as county or block codes or some population counts by area.

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

CEN07 receives address data from internal Census Bureau systems, the U.S. Postal Service (USPS) and Census Bureau Field operations. This data populates the Master Address File (MAF)/Topologically Integrated Geographic Encoding and Referencing (TIGER) database. CEN07 IT systems will receive this data and tabulate the information for various Census Bureau statistical programs.

(c) any information sharing conducted by the system

CEN07 shares information within the Census Bureau with the following IT systems: CEN05, CEN08, CEN09, CEN13, CEN15, CEN19, CEN21, CEN36.

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

Title 13 U.S.C. 6 and 193

(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	
b. Taxpayer ID		f. Driver's License	
c. Employer ID		g. Passport	
d. Employee ID		h. Alien Registration	
		i. Credit Card	
		j. Financial Account	
		k. Financial Transaction	
		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		g. Date of Birth	
b. Maiden Name		h. Place of Birth	
c. Alias		i. Home Address	X
d. Gender		j. Telephone Number	
e. Age		k. Email Address	
f. Race/Ethnicity		l. Education	
		m. Religion	
		n. Financial Information	
		o. Medical Information	
		p. Military Service	
		q. Physical Characteristics	
		r. Mother's Maiden Name	
s. Other general personal data (specify):			

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

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints		d. Photographs	
b. Palm Prints		e. Scars, Marks, Tattoos	
c. Voice Recording/Signatures		f. Vascular Scan	
		g. DNA Profiles	
		h. Retina/Iris Scans	
		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):					

Other Information (specify)
Geocodes, GPS coordinates, zip codes, county codes, state codes

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		Hard Copy: Mail/Fax	Online
Telephone		Email	
Other (specify):			

Government Sources			
Within the Bureau	X	Other DOC Bureaus	Other Federal Agencies
State, Local, Tribal	X	Foreign	X
Other (specify): The Social, Economic, and Housing Statistics Division (SEHSD) provides CEN07 with an edited extract of the Administrative Records address file. The file is an edited IRS file (addresses only, per the information above in 1.1).			

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

<input checked="" type="checkbox"/>	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): Information is collected in support of the Address Matching and Geocoding operation. This is a Census Bureau operation that attempts to achieve geocodes for addresses.			

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 Census Bureau partners with Tribal, Federal, State, and local governments and commercial entities to acquire addresses and mapping data for the communities they serve, as well as government entity boundary data.

The PII that is collected, maintained, or disseminated is necessary to develop the geographic framework (maps, geocodes, etc.). This information is collected in support of the Address Matching and Geocoding operation. This is a Census operation that attempts to achieve geocodes for addresses.

The information in CEN07 is in reference to members of 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	<p>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> <p>CEN07 connects with a number of IT systems within the Census Bureau (i.e. CEN05, CEN08, CEN09 (Cloud Services), CEN13, CEN15, CEN19, CEN21, and CEN36) and receives information from CEN01 and various state, local and tribal entities, and other federal agencies.</p> <p>CEN07 IT systems 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 facilities that house Information Technology systems. Census also deploys an enterprise Data Loss Protection (DLP) solution as well.</p>
	<p>No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.</p>

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.)*

	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: The data is collected for statistical purposes and there is no opportunity to decline providing the data.

- 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: 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: The data is collected for statistical purposes. Data may be updated if the Census Bureau contacts a respondent to update information.

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 addition 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): <u>July 11, 2019</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).
	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 BII/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 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 <i>(list all that apply)</i> :
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
X	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-029-10-05, item # F: Geographic Products and Output
	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 all U.S. housing units, therefore, a serious or substantial number of individuals would be affected if there was loss, theft or compromise of the data.
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/BII in this IT system or the PII/BII itself may result in serious harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII in this IT system is collected under the authority of Title 13 and protected by Title 13 confidentiality. Violation may result in serious penalties.
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 geographic program area, regional offices, and survey program offices, etc. Access is only allowed outside of the physical locations owned by the Census Bureau with a secure connection e.g., Virtual Desktop Interface. 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.