Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Associate Director for Decennial Census Program (ADDCP)
Decennial

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

BYRON CRENSHAW
Digitally signed by BYRON CRENSHAW
Date: 2023.09.20 17:09:38 -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/ADDCP Decennial

Unique Project Identifier: 006-000400400

Introduction: System Description

Provide a brief description of the information system.

Decennial is a collection of applications, technologies, and supporting infrastructure established to support the Decennial Census Programs' mission. Applications support data collection and processing, data management and reporting, content security and Census close out activities.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

Decennial manages the development and implementation of decennial census applications and systems utilized by the Decennial Census Program to produce statistics and consists of applications and systems that collect, maintain and process, and/or disseminate data collected from decennial census respondents and decennial census personnel. These applications and systems process response data from census tests and Decennial Census operations and/or perform quality assurance mechanisms for various census operations.

Applications and systems that collect, maintain, process, and/or disseminate PII include:

Control and Response Data System (CaRDS) - CaRDS provides sample design and Universe determination for the Decennial Census.

Decennial Response Processing System (DRPS) - DRPS provides Auto-coding, Clerical coding, Data editing and imputation for the Decennial post data collection response processing. Additionally, it creates Decennial Response Format (DRF), Census Unedited File (CUF) and Census Edited File (CEF) files.

Decennial Budget Integration Tool (DBiT) – DBiT is used by the Decennial Budget Office (DBO) to perform ongoing cost estimation, budgeting, budget planning, and budget execution management functions required to prepare and execute the Census and beyond, including the Census enterprise.

Network Infrastructure – Network Infrastructure includes hardware and software used to manage the connectivity and communication across Decennial applications and systems.

SAS Foundation – SAS Foundation provides Sampling Criteria, Contact Strategies and Sample for re-interviews, manages the Experiments Program, and verifies the Sample Design File (SDF).

Post-Enumeration Survey (PES) – PES includes the Processing and Control System (PCS) which performs automatic matching, workload control and sampling for Coverage Measurement, Imputation and Estimation System which performs the imputation and estimation for Coverage Measurement, and Clerical Match and Map Update (CMMU) which performs clerical matching activities and map spot updates for Coverage Measurement. The Coverage Measurement program provides estimates of net coverage error and components of census coverage for housing units and people in housing units.

(b) System location

CaRDS, DRPS, DBiT, Infrastructure Services, Network Services, SAS Foundation, and PES are hosted and managed within the Headquarters computer center and/or AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions located in the Eastern and Northwestern parts of the United States.

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

CaRDS, DRPS, DBiT, Network Services, SAS Foundation, and PES interconnects internally with systems within the Census Bureau which include

- OCIO Field Systems Major Application Systems,
- ADDCP Geospatial Services,
- ADDP Demographic Surveys,
- OCIO Commerce Business System (CBS),
- OCFO Budget Systems,
- OCIO Enterprise Data Lake (EDL),
- ADRM Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI),
- ADDCP American Community Survey and Office, and
- ADEP Economic Programs.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

CaRDS, DRPS, Network Services, SAS Foundation, and PES support the collection, monitoring, and processing response data from census tests and Census operations and perform quality

assurance mechanisms for various census operations. Data collection is used to produce statistics.

DBIT – Manages and tracks budget requests.

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

Information in Decennial applications and systems are retrieved by using PII information identified that pertains to authorized users using internal web applications, secure databases, and managed file transfer servers.

Information contained within the applications and systems are not available to the public.

Only authorized Census Bureau federal employees and contractors with a need-to-know have access to the applications. These authorized users' interface with the information contained within the applications and systems using authorized internal web applications, file servers, and/or databases that are protected with a multi-layer security approach. This approach includes the deployment of internal technologies to safeguard data and ensure privacy as well as mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

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

Information is transmitted to and from CaRDS, DRPS, Infrastructure Services, Network Services, SAS Foundation, and PES using secure point-to-point connections. Files are encrypted and transferred using the service-oriented architecture (SOA) via the Enterprise Service Bus (ESB). The ESB is a configuration based, policy-driven enterprise service bus. It provides highly scalable and reliable service-oriented integration, service management, and traditional message brokering across heterogeneous IT environments. It combines intelligent message brokering with routing and transformation of messages, along with service monitoring and administration in a unified software product.

DBIT receives direct feeds and input from OCIO CBS, OCFO Budget applications, and the user community. Communications is performed and secured to and from the system via the TLS 1.2 standard.

(g) Any information sharing

CaRDS, DRPS, DBiT, Network Services, SAS Foundation, and PES shares information internally with systems within the Census Bureau which include OCIO Field; ADDCP Geospatial Services; ADDP Demographic Surveys; OCIO CBS, OCFO Budget, OCIO EDL, ADRM CEDSCI, ADDCP American Community Survey Office, and ADEP Economic Programs.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The following authorities apply to all of the Decennial applications and systems:

Title 13, U.S.C. Section 6c
Title 13, U.S.C. Section 141
Title 13, U.S.C. Section 193
44 U.S.C. Section 3101
41 U.S.C. 433(d)
5 U.S.C. 301
5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533
Executive Order 9397
Executive Order 12107
Executive Order 12564

As noted, the Census Bureau's programmatic authority is Title 13 of the U.S. Code. Title 13 provides authority to conduct the Bureau's work in addition to providing strong confidentiality protections. Section 9 of Title 13 not only requires that the Census Bureau maintain the confidentiality of the information it collects from decennial census respondents, but also mandates that the Census Bureau may use such information it collects for statistical purposes, and the information cannot be used to a respondent's detriment. The Census Bureau cannot publish data that identifies a particular individual or establishment, because of Title 13.

The Census Bureau leverages its Title 13 authority and obligations in coordination with other federal statutes and mandates for privacy, data security, transparency, and accountability, including the Privacy Act, the E-Government Act of 2002, FISMA, and the Paperwork Reduction Act as well as federal standards and guidance promulgated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

All Decennial applications and systems are classified as 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 in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

__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.

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	X

f. Race/Ethnicity	X	m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Decennial applications and systems process response data (general personal data as marked above) from census tests and Census operations. In addition, they serve as quality assurance mechanisms and perform analysis for various census operations. DBIT is the Decennial financial management system that uses contract and user input for Census budget purposes.					

Work-Related Data (WRD)[1]					
a. Occupation		e. Work Email Address	X	i. Business Associates	X
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
Other work-related data (specify): DBIT is the Decennial financial management system that uses contract and user input for Census budget purposes.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints[2]		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): N/A					

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

Other Information (specify)
N/A

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): N/A					

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

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

2.3 Describe how the accuracy of the information in the system is ensured.

All Decennial applications and systems use a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (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, data validation controls to ensure accuracy of information.

Information processed by the Census is validated for accuracy in numerous ways. The processing of the Census unedited and Census Edited files are scrutinized during testing for content accuracy through reviews from the Population (POP) division. POP will assess and notify the affected program areas of discrepancies before information is further processed. Code is updated and information processing is validated through testing to further support information accuracy.

In addition, procedures are in place to ensure that sensitive information is not inadvertently released. As a final stop, the information is reviewed by the Disclosure Avoidance division to ensure that sensitive data is not unintentionally released to the public.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act. *As the Census Bureau gets closer to the 2030 Census, a a new request to get a new clearance number. will be submitted.

2.5 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): N/A			

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			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	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).

CaRDS, DBIT, Network Services, SAS Foundation, and PES: The PII collected, maintained, and/or disseminated by these applications and systems is **in reference to members of federal employee/contractors and the public**. Federal employee/contractor information is maintained to support **administrative matters** including decennial budget activities, access controls and audit logging activities. Data collection from the public is used to **produce national statistical information**.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

Decennial applications and systems adhere to the Information Technology Security Program Policy as it relates to handling, retaining, and disposing collected information. 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 Data Loss Prevention (DLP) solution as well.

Information will be retained in the Decennial applications and systems for the duration of the Census operations and then disposed of following NIST sanitation guidance.

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			

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Federal agencies		X	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): N/A			

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.[4]
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: CaRDS, DRPS, DBiT, Network Services, SAS Foundation, and PES interconnects internally with systems within the Census Bureau which include • OCIO Field Systems Major Application Systems, • ADDCP Geospatial Services, • ADDP Demographic Surveys, • OCIO Commerce Business System (CBS), • OCFO Budget Systems, • OCIO Enterprise Data Lake (EDL), • ADRM Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI), • ADDCP American Community Survey and Office, and • ADEP Economic Programs A multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (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. 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.

[4] External agencies/entities are required to verify with the Census Bureau any re-dissemination of PII/BII to ensure consistency with the MOU/inter-agency agreement and the appropriate SORN

6.4 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): N/A			

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.html In addition, a Privacy Act statement is also provided to applicants during the onboarding process.	
	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: 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. However, PII is protected pursuant to Title 13. For DBiT, information is being pulled from contracts and Active Directory; there is not an opportunity to decline at this level.

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. However, PII is protected pursuant to Title 13. For DBiT, information is being pulled from contracts and Active Directory; there is not an opportunity to consent to particular uses at this level.

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For DBiT, Individuals can review their information and provide updates to their information by submitted a Privacy Act request to the Census Bureau.
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.

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 additional 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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): June 30, 2023. ☐ 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 (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC 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): Section 9 of Title 13 requires that the Census Bureau to maintain the confidentiality of the information it collects from decennial census respondents. In addition, it also mandates that the Census Bureau may use such information it collects for statistical purposes, and the information cannot be used to a respondent's detriment. The Census Bureau cannot publish data that identifies a particular individual or establishment, because of Title 13. The Census Bureau leverages its Title 13 authority and obligations in coordination with other federal statutes and mandates for privacy, data security, transparency, and accountability, including the Privacy Act, the E-Government Act of 2002, FISMA, and the Paperwork Reduction Act as well as federal standards and guidance promulgated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

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 Data Loss Prevention solution as well.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

_X___ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(list all that apply)*: Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/CENSUS-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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: Nl-29-05-01, N1-29-10-5, GRS 1.3, GRS 3.1, GRS 5.6 item 181
	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 Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII collected can be directly and indirectly used to identify individuals.
X	Quantity of PII	Provide explanation: The collection is for the Decennial Census, therefore; a severe or substantial number of individuals would be affected if there was loss, theft or compromise of the data. This could affect Decennial Census response rates and have a long-term effect on the Nation's population count. Severe collective harm to the USCB's reputation, or cost to the USCB 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 PII in this IT system or the PII itself may result in severe harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII collected is required to be protected in accordance with 5, U.S.C (552a) and 13, U.S.C, section 9.
X	Access to and Location of PII	Provide explanation: 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. PII is also located on U.S. Census Bureau authorized vendor

		systems. Access is limited to those with a need-to-know for authorized U.S. Census Bureau contractors and employees.
	Other:	Provide explanation: n/a

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The collection of PII is required for the Census, therefore, a severe or substantial number of individuals would be affected if there was loss, theft, or compromise of the data. This could affect Census response rates and have a long-term effect on the Nation's population count, negatively impact appropriations of Federal tax dollars and apportionment of representation in Congress and jeopardize the reputation of the Census Bureau.

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 Data Loss Prevention solution as well and requires all individuals to complete annual awareness training.

12.2 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.

12.3 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.