Template Version Number: 01-2021

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

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

Reviewed by: Byron A. 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: 2023.01.25 12:42:35 -05'00'

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

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

Unique Project Identifier: 006-000400500

Introduction: System Description

Provide a brief description of the information system.

The Associate Directorate for Demographic Programs (ADDP) is composed of a collection of application components that support the Demographic Directorate business functions. These applications provide users with the ability to develop, collect, analyze, model, and disseminate demographic data. The application components inside the Demographic Statistical Data Processing system are comprised of ongoing work done on Linux machines across five distinct Divisions within the Demographic Directorate. They are as follows: the Social, Economic, & Housing Statistics Division (SEHSD), the Population Division (POP), the Demographic Statistical Methods Division (DSMD), the Demographic Systems Division (DSD), and the Associate Director for Demographic Programs (ADDP).

Address the following elements:

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

The U.S. Census Bureau's Demographic Programs Directorate (DEMO) Demographic Census, Surveys, and Special Processing System is an IT system comprised of a collection of major and minor applications that support the Demographic Directorate business functions.

(b) System location

All DEMO components reside on servers located within the Census Bureau's Bowie Computer Center (BCC).

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

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

- Office of the Chief Information Officer (OCIO) Data Communications system
- Office of the Chief Information Officer (OCIO) Network Services system

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

- Office of the Chief Information Officer (OCIO) Data Communications system
- Office of the Chief Information Officer (OCIO) Network Services system

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

- Associate Director for Economic Programs (ADEP) Economic Census and Surveys and Special Processing
- Associate Director for Research and Methodology (ADRM) Center for Enterprise Dissemination (CED)
- Office of the Chief Information Officer (OCIO) Enterprise Applications
- Associate Director for Decennial Census Programs (ADDCP) American Community Survey Office
- Office of the Chief Information Officer (OCIO) Field Systems Major Application System
- Office of the Chief Information Officer (OCIO) Centurion
- Associate Director for Decennial Census Programs (ADDCP) American Geography
- Associate Director for Decennial Census Programs (ADDCP) American Decennial
- Associate Director for Economic Programs (ADEP) Longitudinal Employer-Household Dynamics (LEHD)
- Associate Director for Economic Programs (ADEP) Economic Applications Division (EAD) Windows Applications System

DEMO also interconnects with external IT systems for the purpose of statistical data collection and processing. Each external interconnection has a different function and purpose as described below:

The interconnection between DEMO and the Bureau of Labor Statistics (BLS) is used to transmit data between Census Bureau Special Sworn Status (SSS) individuals located at BLS and SSS BLS agents located at the Census Bureau in support of the Current Population

Survey (CPS), American Time Use Survey (ATUS), and Consumer Expenditure Survey (CES).

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

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

The interconnection between DEMO and the National Center for Health Statistics (NCHS) is used to make data available from Census Bureau resources to return processed data to NCHS (using the Centers for Disease Control and Prevention (CDC) Secure Access Management System (SAMS)).

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

Personally identifiable information (PII) is collected through various demographic data surveys, focus groups/cognitive interviews, methodological studies, IT systems, and programs to produce national statistical information.

The data is used to calculate and process the statistical data input for the purpose of creating statistical information and reports (i.e., Annual household and group quarters' population estimates by age, sex, race, and origin for counties).

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

- Face-to-face interviews conducted by field representatives (FRs) using Computer Assisted Personal Interview (CAPI) on Field IT systems;
- Telephone interviews conducted by centralized interviewers using Computer Assisted Telephone Interview (CATI) (Field) or by FRs conducting decentralized telephone interviews using CAPI;
- Web-based interviews by respondents. Respondents use a web-based application

instrument that resides on the Census Bureau network via Centurion or Qualtrics. Respondents use their personal computers to access Centurion or Qualtrics.

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

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

Files are identified with either a Case ID or control number, or by a personal identifier (e.g. last four digits of Social Security Number (SSN)) for certain surveys or special research projects. The specified Case ID, control number, or personal identifier is used to retrieve the individual case within a file.

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

The information is collected/transmitted using Federal Information Processing Standards (FIPS) 140-2 compliant encryption.

(g) Any information sharing conducted by the system

There is PII being shared as follows:

- DEMO shares information with Economic Census and Surveys and Special Processing, Geography, Decennial, CED, LEHD, Enterprise Applications, American Fact Finder - Data Access & Dissemination Systems (AFF-DADS), and American Community Survey Office. In addition, DEMO receives information from CED, American Community Survey Office and EAD Windows Applications System.

- The Census Bureau provides access to staff at HUD with SSS for AHS and other surveys they sponsor via VDI in their Survey Sponsor Data Center. The same is true of the HHS, HRSA and HRSA's MCHB or the National Survey of Children's Health (NSCH), the HPD, and HHS and HRSA's National Center for Health Workforce Analysis for the National Sample Survey of Registered Nurses (NSSRN).

- The Census Bureau provides some BLS staff access to CPS, ATUS, and CE data on a DEMO server. BLS staff have SSS to have Census Bureau accounts to access the server. Consumer Expenditure staff at BLS access CPS data for weighting purposes.

- The Census Bureau sends data files to NCHS for the National Ambulatory Medical Care Survey (NAMCS), the National Hospital Ambulatory Medical Care Survey (NHAMCS) and National Health Interview Survey (NHIS). Data transfers are

conducted through CDC 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 Private School Survey (PSS), the National Teacher and Principal Survey (NTPS), the Teacher Follow-up Survey (TFS), the Principal Follow-Up Survey (PFS), the School Pulse Panel (SPP), and the National Training, Education, and Workforce Survey (NTEWS) seeded sample. Data transfers are conducted through the Institute of Education Sciences (IES) Members Site.

- The Census Bureau provides restricted access to staff of the National Center for Science and Engineering Statistics (NCSES) at the National Science Foundation (NSF) for the National Survey of College Graduates (NSCG) and the National Training, Education, and Workforce Survey (NTEWS). Staff of the National Center for Education Statistics (NCES) are also provided restricted access for the NTEWS. Staff with access have SSS and connect via the Census Bureau VDI.

- The Census Bureau provides restricted access to BJS staff for the National Crime Victimization Survey (NCVS) and related NCVS supplements. Staff with access have SSS and connect via the Census Bureau VDI.

- The Census Bureau provides restricted access to internal Household Pulse Survey data to staff with SSS access from the United States Department of Agriculture Economic Research Service (USDA-ERS) through the Bureau's internal research environment (IRE).

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

13 USC Sections 8(b), 23(c), 182, 193, 196

(i) The Federal Information Processing Standards (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):					

____ 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*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		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:

The last 4-digits of the SSN is used in admin records matching to NHIS.

The justification for the necessity of collecting this information, taken from the latest approved Office of Management and Budget (OMB) Information Collection Request (ICR) supporting statement is below:

Social Security Number and Health Insurance Claim Number: The last four digits of the (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 identifying 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 residence, 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 SSN is also used by the Medical Expenditure Panel Study to help track the location of respondents who have changed residence since their NHIS interview. 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	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion	X		
u. Other general personal data (specify): sexual orientation, gender identity, federal stimulus payments (if applicable), and federal tax credits.					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): Paradata					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording	X	h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height	X	n. Retina/Iris Scans	
e. Photographs		j. Weight	X	o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Eye tracking technology which captures a photograph of the exterior of the subjects' eyes[1].					

[1] Eye tracking technology does not scan the iris or retina of the eye. It captures a photograph of the exterior of the eye. The Census Bureau will also use an eye tracking technology to help evaluate the attentiveness and focus of research participants when reviewing Census Bureau questionnaires. The eye tracking technology uses a light source to illuminate the eye causing highly visible reflections. An image of the eye is captured by a camera and is used to identify the reflection of the light source on the cornea (glint) and in the pupil. Census Bureau researchers

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		f. 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	X
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 Describe how the accuracy of the information in the system is ensured.

The survey instruments include questions to verify the sample person or sample address before asking the remaining questions in the survey instrument to help ensure we are collecting data from the intended sample person/address. Survey program areas ensure the accuracy of the information collected, processed, and disseminated. Quality control and review processes, both automated within the systems, and manual reviews of system outputs are used to ensure the accuracy and quality of the data and information produced within the system. Ongoing system development practices (i.e., code reviews, configuration management, etc.), ensure system development meets requirements.

The accuracy of the information on DEMO servers is ensured via FIPS 140-2 compliant algorithms.

will use this information to calculate a vector formed by the angle between the cornea and pupil reflections. This information is then used to calculate the gaze direction. The eye tracking technology, including eye images captured by the Census Bureau are done on secure government computers and handled in a manner consistent with federal data protection requirements as detailed in this PIA.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 2528-0017, 1220-0175, 1220-0187, 0607-0354, 1220-0050, 0970-0416, 3045-0139, 0660-0221, 1220-0153, 0607-0049, 1220-0100, 1220-0104, 0607-0610, 1018-0088, 0536-0043, 0607-0179, 1121-0317, 0920-0234, 3064-0167, 1121-0111, 0920-0278, 1850-0768, 0920-0214, 3145-0141 ,0607-0990, 1850-0598, 0607-0757, 1121-0260, 1850-0641, 0607-0464, 1121-0184, 0607-0977, 2528-0013, 3135-0136, 0607-0980, 1850-0761, 1121-0302, 1220-0044, 0925-0368, 1220-0102, 1220-0176, 1850-0617
	No, the information is not covered by the Paperwork Reduction Act.

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):			

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 SIPP and Consumer Expenditure Survey (CES); in the future DEMO may incorporate CARI for additional 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			
For a Computer Matching Program		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	X	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).

To improve Federal services online: The statistical data products created and disseminated by the DEMO systems provide valuable information to other federal, state and local governments, other private organizations and the general public. This improves online Federal Services and customer satisfaction by effectively and efficiently making this critical data freely available in easy to find and use methods.

For statistical purposes (i.e., Censuses/Surveys): PII is collected from the public through various demographic data surveys, programs, focus groups/cognitive interviews, or methodological studies to produce national statistical information.
The data is used to calculate and process the statistical data input for the purpose of creating statistical information and reports (e.g., Annual household and group quarters' population estimates by age, sex, race, and origin for counties, etc.).
The information that is collected in this system is from members of the public and DOC employees.

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.

In addition, the 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 the National Institute of Standards and Technology (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 hypertext transfer protocol secure (HTTP(S)) for Census Bureau 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

The Census Bureau Information technology systems also follow NIST standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau 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. The census Bureau also deploys an enterprise email Data Loss Prevention (DLP) solution.

The information in DEMO is handled, retained and disposed of in accordance with appropriate federal record schedules.

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	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 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.
	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: DEMO transmits/receives data required for statistical data collection and processing to/from these IT systems: • ADEP Economic Census and Surveys and Special Processing • ADRM Center for Enterprise Dissemination (CED) • OCIO Enterprise Applications • ADDCP American Community Survey Office • OCIO Field Systems Major Application System • OCIO Centurion • ADDCP Geography • ADDPC Decennial • ADEP Longitudinal Employer-Household Dynamics (LEHD) • ADEP EAD Windows Applications System DEMO also interconnects with external IT systems for the purpose of statistical data collection and processing. Each external interconnection has a different function and purpose as described below: The interconnection between DEMO and the Bureau of Labor Statistics (BLS) is used to transmit data between Census Bureau Special Sworn Status (SSS) individuals located at BLS and SSS BLS agents located at the Census Bureau in support of the Current Population Survey (CPS), American Time Use Survey (ATUS), and Consumer Expenditure Survey (CES). Utilizing virtual desktop infrastructure (VDI), Census Bureau provides Department of Housing and Urban Development (HUD) staff with Special Sworn Status (SSS) access to the American Housing

	Survey (AHS) and other surveys they sponsor. The same is true for U.S. Department of Health and Human Services (HHS) Health Resources and Services Administration (HRSA), HRSA's Maternal and Child Health Bureau (MCHB), HRSA's National Center for Health Workforce Analysis (NCHWA), the New York City Department of Housing Preservation and Development (HPD), the Bureau of Justice Statistics (BJS), the National Center for Education Statistics (NCES), and the staff of the National Center for Science and Engineering Statistics (NCSES) at the National Science Foundation (NSF). These entities gain access to these data utilizing VDI. The interconnection between DEMO and the National Center for Health Statistics (NCHS) is used to make data available from Census Bureau resources to return processed data to NCHS (using the Centers for Disease Control and Prevention (CDC) Secure Access Management System (SAMS)). The DEMO 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 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 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.

6.4 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):			

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: DEMO 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 System of Record Notice (SORN) 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. Exception: SIPP has a Respondent Identification Policy (RIP) question that allows an individual respondent to decline sharing their PII as dependent data in the next interview, though it is still part of the dataset in the interview it was collected.

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 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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 6/29/22 ☐ 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): 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. *(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/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 NIST standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census that contains, transmits, or processes PII has a current ATO and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. Census also deploys an enterprise email DLP 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)*: COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html COMMERCE/CENSUS-7, Demographic Survey Collection (Non-Census Bureau Sampling Frame) http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.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: N1-29-99-5 N1-29-89-3 NC1-29-85-1 NC1-29-79-7 GRS 3.1 GRS 3.2 GRS 4.1 N1-029-12-001 GRS 5.1 and 5.2
	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 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 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, 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 PII may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII collected is required to be protected in accordance with Title 13 Section 9 and organizational policy.

		Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: PII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access 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 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.)

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know.

The 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

The Census Bureau Information technology systems also follow NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current 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 and requires Census Bureau information system users to complete annual Data Stewardship 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.