DATA USE AGREEMENT
Between the
U.S. CENSUS BUREAU
and the
DEPARTMENT OF HOMELAND SECURITY/USCIS OFFICE OF PERFORMANCE AND QUALITY

In order to ensure the integrity, security, and confidentiality of information maintained by the Department of Homeland Security (DHS)/Office of Performance and Quality (OPQ) and to permit appropriate disclosure and use of such data as permitted by law, the DHS/OPQ and the U.S. Census Bureau (Census Bureau) enter into this Data Use Agreement (Agreement) to comply with the following specific paragraphs:

1. This Agreement is by and between the DHS/OPQ and the Census Bureau, a component of the U.S. Department of Commerce. This Agreement is by and between the DHS/OPQ and the Census Bureau, a component of the U.S. Department of Commerce. This agreement does not obligate the funds of either party to the agreement. Each party will assume its own costs; and if funding transfers are required, they will be executed through written amendment to the agreement. This Agreement shall become effective as of the date of the last signatory in items 19 and 20 and will end five years from that date. This Agreement shall become effective as of the date of the last signatory in items 19 and 20 and will end five years from that date.

2. This Agreement addresses the conditions under which the DHS/ OPQ will disclose and the Census Bureau will obtain and use the DHS/ OPQ data files specified in item 7. The terms of this Agreement can be changed only by a written modification to this Agreement, signed by both parties, or by the parties adopting a new agreement. This Agreement and its attachments must be formally reviewed whenever a Federal statute is enacted that materially affects the substance of the Agreement, or at least every three years to assure its currency. The review will be conducted in the Census Bureau by the appropriate Associate Director and by the appropriate DHS/ OPQ representative. The result of the review will be a decision agreed to by both agencies to continue the Agreement unchanged, an amendment to continue the Agreement with specified changes, or a cancellation of the Agreement. Any amendments to the Agreement will require the review and approval of the DHS/OPQ designee and the appropriate Census Bureau Associate Director or their designee. The parties agree further that instructions or interpretations issued to the Census Bureau concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the DHS/OPQ point of contact specified in item 5, or the DHS/OPQ signatory to the Agreement shown in item 20.

3. The Census Bureau's access to the data files is authorized under Title 13, United States Code (U.S.C.), Section 6. The confidentiality of the DHS/OPQ data is guaranteed under Title 13, United States Code, Section 9; and Title 5, United States Code, Section 552a(b). Only sworn Census Bureau employees and

individuals with Census Bureau Special Sworn Status (SSS) will have access to the Title 13-protected data files. The DHS/OPQ shall make the specified information available to the Census Bureau pursuant to Title 5, U.S.C., Section 552a(b)(4).

4. The parties mutually agree that the following named individual is designated as "Custodian" of the files on behalf of the Census Bureau and will be personally responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The Census Bureau agrees to notify the DHS/OPQ within fifteen (15) days of any changes of custodianship. The parties mutually agree that the DHS/OPQ may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

Custodian: J. Trent Alexander
Center for Economic Studies
U.S. Census Bureau
HQ-(b) (6)
4600 Silver Hill Road
Suitland, MD 20746
301-763-9810 Phone
301-763-4310 Fax
J.Trent.Alexander@census.gov (Email)

Processing Sites: Bowie Computer Center, Bowie, MD
Suitland Federal Reservation, Suitland, MD

5. The parties mutually agree that the following named individual will be designated as "point of contact" for the Agreement on behalf of the DHS/OPQ.

Chief, Office of Performance and Quality
US Citizenship and Immigration Services
Phone No.: (202) 272-1258
Email: (b) (6)

6. In furnishing the data files specified in item 7, the DHS/OPQ relies upon the Census Bureau's representation and warranty that such data files will be used solely for the purposes of developing benchmark statistics for the components of net international migration which are vital to the Census Bureau's Population Estimates and Population Projections Programs, and to inform immigration research at the Census Bureau.

The Census Bureau represents and warrants further that, the Census Bureau shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access

to the original data covered by this Agreement to any unauthorized person or entity. The Census Bureau agrees that within the Census Bureau organization, access to the original data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this section.

7. The DHS/OPQ shall prepare and forward to the Census Bureau on DVD/CD ROM that is compacted with WinZip and password protected the following specific data file:

- **Legal Permanent Resident (LPR) File**

The request for the LPR data is for the period of Federal Fiscal Year (FY) 2015 (starting on October 1, 2014) to FY 2019 (ending on September 30, 2019). These data will be supplied annually on encrypted DVD/CD-ROM. For each subsequent year, a request will be made for an annual file. File updates will be requested where applicable.

Data elements included on these files are provided in the standard file layouts in Attachment 2. Notwithstanding any other provisions of this Agreement, the records shall be treated in a manner that will assure that individually identifiable data will be used only for statistical purposes and will be accessible only to authorized persons. Authorized persons include Census Bureau employees and individuals with Census Special Sworn Status, (including contract employees) who are working on projects approved by the Census Bureau, and have sworn the Census Bureau's oath of confidentiality.

8. The parties mutually agree that the aforesaid files, and any derivative files that contain identification of individuals may be retained by the Census Bureau for 10 years after receipt. This complies with the Census Bureau's record retention schedule that states that the retention period for original files from outside sources be destroyed when 2 years old or as contract specifies. The Census Bureau agrees to notify the DHS/OPQ within 30 days of the completion of the purpose specified in item 6 if the purpose is completed before this aforementioned retention period. Upon such notice or at the end of the above-mentioned retention date, whichever occurs sooner, the Census Bureau will destroy such data. When the Census Bureau destroys the data, the Census Bureau agrees to certify the destruction of the files in writing within 30 days of receiving the DHS/OPQ's instructions. A statement certifying this action must be sent to the DHS/OPQ. The Census Bureau agrees that no data from the DHS/OPQ records, or any parts thereof, shall be retained when the aforementioned files are destroyed unless authorization in writing for the retention of such files has been received from the point of contact as identified in item 5 of this Agreement. The Census Bureau acknowledges that stringent adherence to the aforementioned retention period is required, and that the Census Bureau shall ask the DHS/OPQ for instructions under this paragraph if instructions have not been received within 30 days after the retention period ends.

The extended retention period of 10 years is requested in order to allow for

research and development of longitudinal modeling techniques and survey validation associated with the creation of estimates of the net migration of the foreign-born, and benchmark estimates of the foreign-born by legal status. Aggregate statistics modeled from records provided by the DHS/OPQ and other agencies will be applied to the Census Bureau estimates of the net migration of the foreign-born in order to improve existing methodology.

9. The Census Bureau agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data supplied by DHS/OPQ and to prevent unauthorized use of, or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Systems, and the E-Government Act of 2002 which sets forth regulations and guidelines for security documentation for automated information systems in Federal agencies.

The Census Bureau acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable or deducible information derived from the file(s) specified in item 7 is prohibited. Further, the Census Bureau agrees that the data must not be physically moved or transmitted in any way from the site(s) indicated in item 4 without prior written approval from the DHS/OPQ.

The Census Bureau maintains secure computer facilities located in secured buildings at the Bowie Computer Center, in Bowie, Maryland and secured facilities at Census Headquarters on the Suitland Federal Reservation in Suitland, Maryland. Computer systems that will store the DHS/OPQ data are located at the Bowie Computer Center.

Security guards and electronic card keys control access to the Bowie and Suitland facilities. Controls on the computers are outlined in sensitive security plans CEN01 Data Communications, CEN11 Demographic Census, Surveys, and Special Processing, CEN16 Network Services, and CEN17 Client Services. Access to the computer databases is strictly limited to authorized individuals for the uses described above.

The Bowie Computer Center is connected to Census Headquarters via dedicated fiber cable (dark fiber). The Census Bureau controls both ends of the circuit. This allows for secure transmission of data without encryption. Analysts and programmers at Census Headquarters access data stored on computer systems in the Bowie Computer Center via these lines. Access controls on all the computers include individual accounts with unique passwords as well as Access Control Lists.

The Census Bureau computer systems follow (but are not limited to) the requirements of the E-Government Act of 2002, Section 3544, which describes

Federal Agency responsibilities for providing information security protections are commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. This includes conforming to the standards and scope of security established in OMB Circular A-130, Appendix III, which establishes computer security plans for sensitive systems using the U.S. Department of Commerce "NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems Rev.l (February 2006)," and meeting the minimum requirements of the "Recommended Security Controls for Federal Information Systems, NIST SP 800-53 Rev.I, December 2006."

Notwithstanding the preceding paragraph or other provisions of this Agreement, the Census Bureau understands and agrees that no individual entity shall be identified in publicly released information.

Any user aware that personally identifiable information received from DHS/OPQ under this Agreement/DUA may have been lost or disclosed to any unauthorized persons must notify Chief, DHS/OPQ, at (phone no.) or (email address) and the BOC CIRT at 301-763-5141 (7:30 am to 5:00 pm, 1-877-343-2010 (anytime), or BOC.CIRT@census.gov within one (1) hour and to cooperate fully in the Federal security incident process.

10. The Census Bureau agrees that authorized representatives of the DHS/OPQ will be granted access to premises where the aforesaid files are kept for inspecting security arrangements to confirm whether the Census Bureau is in compliance with the security requirements specified in paragraph 9. Said access will be granted to the authorized representatives upon swearing the Census Bureau's oath of confidentiality.

11. The Census Bureau and DHS/OPQ further agree that the Census Bureau will provide full Title 13 confidentiality protection to identities of individuals in all the items derived from the files noted in item 7.

12. The inclusion of linkage of specific files in this Data Use Agreement approved in accordance with item 6, is considered express written authorization from the DHS/OPQ.

13. The Census Bureau understands and agrees not to extend the scope of use of the original data files beyond the uses described herein without prior written approval by the designated DHS/OPQ representative. The DHS/OPQ acknowledges that derivative products that no longer contain DHS/OPQ data items are not covered by this prohibition.

14. The Census Bureau agrees that in the event the DHS/OPQ determines or has a reasonable belief that the Census Bureau has made or may have made disclosure of information contained in the aforesaid file(s) without authorization by the DHS/OPQ Executive Director, the DHS/OPQ in its sole discretion and to the extent permitted by law, may require the Census Bureau to: (a) promptly investigate and report to the DHS/OPQ the Census Bureau's determinations regarding any alleged or actual unauthorized disclosure; (b) promptly resolve any problems identified by the investigation; (c) submit a formal response to an allegation of unauthorized disclosure; and (d) submit a corrective action plan with steps designed to prevent any future unauthorized disclosures. The Census Bureau understands that, as a result of the DHS/OPQ's determination or reasonable belief that unauthorized disclosures have taken place; the DHS/OPQ may refuse to release further DHS/OPQ data to the Census Bureau for a period of time to be determined by the DHS/OPQ or may unilaterally and immediately terminate this agreement.

15. The Census Bureau acknowledges that criminal penalties may be imposed:

- On a Census employee for wrongful disclosure of confidential Census information under Title 13, United States Code (U.S.C.), Section 214, as revised by Title 18, U.S.C., Section 3551 et seq., for a fine of up to $250,000, imprisonment of up to 5 years, or both.

- Under the Privacy Act (5 U.S.C. Section 552a(i)(1) and (3)) may apply, if it is determined that the Requestor or Custodian, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretense and/or knowingly and willfully discloses the files(s). Any person found guilty under the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000.

- Under 18 U.S.C. Section 641, which provides that if it is determined that the Census Bureau, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s) or received the file(s) knowing that they were stolen or converted, they shall be fined not more than $250,000 or imprisoned not more than ten (10) years, or both.

In addition, the Census Bureau may be subject to civil suit under the Privacy Act (5 U.S.C. Section 552a(g)) for damages which occur as a result of willful or intentional actions which violate an individual's rights under the Privacy Act.

Notwithstanding all other provisions of this Agreement, the Census Bureau understands and agrees to the following provisions:

a. This Agreement may be amended at any time by written mutual consent of both parties.

b. Either party may terminate this Agreement upon thirty (30) days' written

notice to the other party.

c. In the event of a dispute between the DHS/OIS and the Census Bureau regarding any part of this Agreement, the dispute may be submitted to non-binding arbitration upon the consent of both the DHS/OIS and the Census Bureau. An election for arbitration pursuant to this provision shall not preclude either party from pursuing any remedy for relief otherwise available.

16. By signing this Agreement, the Census Bureau agrees to abide by all provisions set out in this Agreement for protection of all information contained in the data file(s) specified in item 7, and acknowledges having received notice of potential criminal, administrative, or civil penalties for violation of the terms of the Agreement.

17. On behalf of the Census Bureau, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Amy O'Hara — 7-27-15

Amy O'Hara — Date
Chief, Center for Administrative Records
Research and Applications
U. S. Census Bureau

18. The Custodian, as named in paragraph 4, hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the Census Bureau, and agrees personally and in a representative capacity to comply with all of the provisions of this Agreement on behalf of the Census Bureau.

J. Trent Alexander — 7/27/15

J. Trent Alexander — Date
Assistant Center Chief for Research Support
Center for Economic Studies
U. S. Census Bureau

19. On behalf of the Census Bureau, the undersigned individual hereby acknowledges that the aforesaid Federal agency sponsors or otherwise supports the Census Bureau's request for and use of the DHS/OIS data, agrees to support the DHS/OIS in ensuring that the Census Bureau maintains and uses the DHS/OIS's data in accordance with the terms of this Agreement, and agrees further to make no statement to the Census Bureau concerning the interpretation of the terms of this Agreement and to refer all questions of such interpretation or compliance with the terms of this Agreement to the DHS/OIS officials named in item 20 (or to his or her successor).

For: [signature] 9/10/15

Amy O'Hara Date
Chief, Center for Administrative Records
Research and Applications
U. S. Census Bureau

20. On behalf of the DHS/OPQ, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

[signature] 9/30/15

Date

Chief, Office of Performance and Quality
US Citizenship and Immigration Services
Department of Homeland Security

Enclosures:

Attachment 1: Census Bureau's File Specifications and Requirements for the LPR files
Attachment 2: File Format/File Layout for the LPR files

Attachment 1

FY 2015-2019 Census Bureau File Specifications and Requirements for the Department of Homeland Security/Office of Immigration Statistics

Legal Permanent Resident (LPR) files

Geography:	**National File**
Reference Period:	All records entered or updated between: October 1, 2013 and September 30, 2014* October 1, 2014 and September 30, 2015* October 1, 2015 and September 30, 2016 October 1, 2016 and September 30, 2017 October 1, 2017 and September 30, 2018 October 1, 2018 and September 30, 2019
Delivery Dates:	November 15, 2015 (for both sets with asterisks) November 15, 2016 November 15, 2017 November 15, 2018 November 15, 2019
Data Variables:	**See Attachment 2**
Special Instructions:	Please make sure that the data and variable names/codes are consistent from year to year.
Transfer Media:	DVD/CD-ROM (encrypted) **(Please e-mail Census Bureau Technical Contact Person with password)**
Format:	ASCII
Documentation:	1. Please include the latest codebook (digital preferred), record layout, record count, and the name and telephone number of a technical advisor, if we should have questions. 2. Include responses required in special instructions.
Delivery Method:	Traceable Delivery Service (Federal Express, UPS, etc.)
Mark Shipment:	**DHS – LPR File** **DVD/CD-ROM – DO NOT X-RAY**
Mailing Address for Shipments:	Please e-mail at the time of shipment. Ms. Vickie Kee U.S. Census Bureau CES/Research Support Area CES HQ (b) (6) 4600 Silver Hill Road Suitland, MD 20746 Vickie.lynn.kee@census.gov Ces.dpg.list@census.gov
Census Bureau Technical Contact Person:	Ms. Vickie Kee 301-763-3071 301-763-3072 (staff)

Attachment 2

File Format/File Layout

Item Number	Position in Data File	Item Length	Variable Name
1	1-3	3	Class of admission
2	4-5	2	Class of admission by major category
3	6	1	Prime/Dependent
4	7	1	Type of immigrant
5	8-12	5	Country of citizenship
6	13-16	4	Year of birth
7	17-18	2	Month of birth
8	19-20	2	Day of birth
9	21-22	2	Age
10	23-27	5	Country of birth
11	28-30	3	Occupation
12	31-35	5	Country of last residence
13	36	1	Marital status
14	37	1	Gender
15	38-39	2	In care of Address – State
16	40-44	5	In care of Address – ZIPCode
17	45-47	3	Last Nonimmigrant class of admission
18	48-51	4	Last Nonimmigrant year of admission
19	52-55	4	Decision Date Year
20	56-57	2	Decision Date Month
		Total Length=57	

IMPORTANT NOTE: Please provide consistent country codes from year to year. In the previous files, country codes were not always coded consistently, e.g., Serbia was coded as "SERBI" and also as "SRBIA" resulting in data processing problems.

Enclosure

MODIFICATION 1 TO THE
DATA USE AGREEMENT
BETWEEN THE
U.S. CENSUS BUREAU and
the
DEPARTMENT OF HOMELAND SECURITY/USCIS OFFICE OF PERFORMANCE AND QUALITY
0094-FY15-NFE-0011.001

This document constitutes an amendment to Agreement No. 0094-FY15-NFE-0011.000 between the U.S. Census Bureau (Census Bureau) and the Department of Homeland Security/Office of Performance and Quality (DHS/OPQ) dated September 30, 2015. The amendment (i) documents the parties' agreement to update the Data Custodian and Delivery Dates of the Legal Permanent Resident (LPR) files. The purpose of the amendment is to:

1. **Replace Number 4., Custodian with the following:**

Custodian: John Moulton
Center for Administrative Records Research and Applications
U.S. Census Bureau
HQ-(b) (6)
4600 Silver Hill Road
Suitland, MD 20746
301-763-8646 Phone
301-763-0271 Fax
John.Richard.Moulton@census.gov (Email)

2. **Replace Attachment 1. with the following:**

Attachment 1

FY 2015-2019 Census Bureau File Specifications and Requirements for the Department of Homeland Security/USCIS Office of Performance and Quality

Legal Permanent Resident (LPR) files

Geography:	**National File**
Reference Period:	All records entered or updated between: October 1, 2013 and September 30, 2014 October 1, 2014 and September 30, 2015 October 1, 2015 and September 30, 2016 October 1, 2016 and September 30, 2017 October 1, 2017 and September 30, 2018 October 1, 2018 and September 30, 2019
Delivery Dates:	May 31, 2016 August 30, 2016 August 30, 2017 August 30, 2018 August 30, 2019 August 30, 2020
Data Variables:	See **Attachment 2**
Special Instructions:	Please make sure that the data and variable

	names/codes are consistent from year to year.
Transfer Media:	DVD/CD-ROM (encrypted) **(Please e-mail Census Bureau Technical Contact Person with password)**
Format:	ASCII
Documentation:	1. Please include the latest codebook (digital preferred), record layout, record count, and the name and telephone number of a technical advisor, if we should have questions. 2. Include responses required in special instructions.
Delivery Method:	Traceable Delivery Service (Federal Express, UPS, etc.)
Mark Shipment:	**DHS – LPR File** **DVD/CD-ROM – DO NOT X-RAY**
	Please e-mail at the time of shipment.
Mailing Address for Shipments:	Ms. Vickie Kee U.S. Census Bureau CES/Research Support Area CES HQ (b) (6) 4600 Silver Hill Road Suitland, MD 20746 Vickie.lynn.kee@census.gov Ces.dpg.list@census.gov
Census Bureau Technical Contact Person:	Ms. Vickie Kee 301-763-3071 301-763-3072 (staff)

All other terms and conditions contained in the original Census Bureau/DHS OPQ Data Use Agreement shall remain the same.

SIGNATURES:

On behalf of the Census Bureau, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

RJ 5/16/16

Ron S. Jarmin — Date

Assistant Director for Research and Methodology
U. S. Census Bureau

On behalf of the DHS/OPQ, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Michael D. Hoefer 5/23/16

Michael D. Hoefer — Date

Chief, Office of Performance and Quality
US Citizenship and Immigration Services
Department of Homeland Security

Enclosure

U.S. Department of Commerce
Bureau of the Census

Privacy Impact Assessment
for the
CEN13 Center for Economic Studies (CES)

Reviewed by: [signature] 4/19/18, 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

LISA MARTIN

Digitally signed by LISA MARTIN
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=LISA MARTIN, 0.9.2342.19200300.100.1.1=13001000105292
Date: 2018.06.26 14:07:58 -04'00'

For Dr. Catrina D. Purvis

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

U.S. Department of Commerce Privacy Impact Assessment
Bureau of the Census, CEN13 Center for Economic Studies (CES)

Unique Project Identifier: 006-000400700

Introduction: System Description

Provide a description of the system that addresses the following elements:

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

The Center for Economic Studies IT System includes data maintained by the Federal Statistical Research Data Centers (FSRDCs), the Center for Economic Studies and the Center for Administrative Records Research and Applications (CARRA). The CEN13 CES IT system covers the personally identifiable information (PII) and Business identifiable information (BII) from each of the centers maintained by the system. The CES data holdings include census and survey data which may contain name, gender, age, date of birth etc. from across the Census Bureau, administrative records from other federal agencies, and proprietary data files from commercial vendors and some non-profits.

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

For internal Census staff users, the Data Management System (DMS) is used to perform management and tracking functions for research proposal and active projects. The DMS is used to track the status and activity of all projects from initial conception through completion and close out.

For external FSRDC users, the CES Management System (CMS) is used to perform management and tracking functions for research proposals and active projects. The CMS is used to track the status and activity of all projects from initial conception through completion and close out. Data is available only to researchers who have received prior approval.

As an example, there may be a researcher wants to conduct an external project using the Census Bureau's 2012 Survey of Business Owners (SBO). Information about the researcher is collected to create an account in CMS; that account is associated with a project that is documented in CMS (e.g. datasets such as SBO), the date pertaining to the of the data (e.g. 2012), other researchers (i.e. research assistant), and the length of the project, (in this example three years). The CMS is used to track all required reviews for the proposal. Once the project and Special Sworn Status (SSS) for the individual is approved, the researcher is provided a badge to access the FSRDC facility and a user account to access the server. The researcher can then proceed to conduct their project. The CMS tracks ongoing activity during the life of the project: who works on the project, annual training for each person, annual reports, and disclosure requests. When the project is completed, the final report from the project and the archival of the project files.

(c) any information sharing conducted by the system

CES CEN13 has ISA ICD's with the following Census systems – data is shared with:

- ADEP ITO Associate Directorate for Economic Programs (CEN36)
- EAD Economic Census and Surveys and Special Processing (CEN03)
- GEO Geography (CEN07)
- DSD Demographic Census, Surveys and Special Processing (CEN11)

CES CEN13 has MOU's or contracts with the following systems external to Census:

- Agency for Healthcare Research and Quality
- Bureau of Labor Statistics
- Department of Energy
- National Center for Health Statistics
- Internal Revenue Service

CES also shares data within the Bureau, with designated Federal agencies, State, Local and Tribal governments and Non-Profit organizations as part of its mission.

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

13 U.S.C., Chapter 5, 8(b), 131, 132, and 182 and 13 U.S.C. 6

(e) 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.
Existing System, No New Security Risks.

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X
c. Employer ID	X	g. Passport		k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*SSNs are often included in administrative records datasets acquired in support of the Census Bureau's Title 13 authority to collect these data. When SSNs are present in these data they serve as one of several components used in a matching or look-up process to assign an anonymized protected identification key (PIK) to the record.					

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

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

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

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

Other Information (specify)

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

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

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

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	X
Third Party Website or Application					
Other (specify): Some data is received from Non-profit organizations					

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

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

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

Section 3: System Supported Activities

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

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

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

Section 4: Purpose of the System

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

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	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): Research, Improvement/support of Census Bureau programs through use of administrative and other non-survey data, Quality assurance, and statistical purposes.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, 1) describe how the PII/BII that is collected, maintained, or disseminated will be used. 2) 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).

Administration and research mission of the CEN13 program for statistical purposes:

For administrative matters:
The PII/BII is used for record linkage. SSNs are used to assign protected identification keys (PIKs) after which SSN and other PII are dropped from the file. After the PIK is assigned, ,files are linked only by PIK. This PII/BII covers members of the public, businesses, contractors and federal employees.

Research, Improvement/support of Census Bureau programs through use of administrative and other non-survey data, Quality assurance, and statistical purposes:
Record linkage using BII and PIKs facilitates research to improve and support existing Census Bureau programs and creation of beta data products. These products use innovative techniques that leverage existing data and reduce the burden on respondents. This PII/BII covers members of the public, businesses, contractors and federal employees.

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	
DOC bureaus		X	
Federal agencies		X	
State, local, tribal gov't agencies		X	
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Data is made available to approved researchers on the RDC and CES internal servers, the researchers are Sworn Census employees, Contractors or Special Sworn Status.	X		

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

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

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: CES CEN13 has shares data with the following Census Bureau systems: • ADEP ITO: Associate Directorate for Economic Programs (CEN36) • EAD: Economic Census and Surveys and Special Processing (CEN03) • GEO: Geography (CEN07) • DSD: Demographic Census, Surveys and Special Processing (CEN11) CES CEN13 receives data from the following Census Bureau systems: • ACSO: American Community Survey (CEN30) • ITMD: Foreign Trade Division Applications (CEN34) • DSCMO-DSSD: Decennial (CEN08) • ASCO: American Community Survey (CEN30) CES also receives data from within the Bureau, designated Federal agencies, State, Local and Tribal governments and Non-Profit organizations as part of its mission. CEN13 uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at

	Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): Special Sworn Status employees of the Census Bureau			

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	
	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.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: When survey is voluntary individuals may decline to provide PII/BII; however in the case of aggregated secondary data there is no interaction with an individual. Survey data are not collected by CEN13 CES.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: When survey is mandatory individuals may not decline to provide PII/BII, and in the case of aggregated secondary data, there is no interaction with an individual. Survey data are not collected by CEN13 CES.

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: When survey is voluntary individuals may consent to particular uses of their PII/BII; however in the case of aggregated secondary data there is no interaction with an individual. Survey data are not collected by CEN13 CES.
X	No, individuals do not have an opportunity to consent to particular	Specify why not: In the case of aggregated secondary data, there is no interaction with an individual. Survey data are not

	uses of their PII/BII.	collected by CEN13 CES.

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: In the case of aggregated secondary data there is no direct contact with the individual.

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: All individual activities within PII systems are logged, access is controlled by Access Control Lists(ACL) and all controls are reviewed in accordance with Audit and Accountability controls and Continuous Monitoring as specified in NIST 800-53 Revision-4. Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 13, 2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	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. (Similar to 6.2, technical controls and leakage management)

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 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 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 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 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 a DLP solution as well.

Section 9: Privacy Act

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: Census-8, Statistical Administrative Records System
X	Yes, a SORN has been submitted to the Department for approval on (date). Census - 4, Economic Survey Collection submitted on 8/24/16
	No, a SORN is not being created.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule:

	GRS 3.1 General Technology Management Records, GRS 3.2 Information Systems Security Records; GRS 4.3 Input Records, Output Records and Electronic Copies. DAA-0029-2014-0005: Records of the Center for Administrative Records Research and Applications.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

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

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

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

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

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

X	Identifiability	Provide explanation: Individual data elements directly identifying unique individuals.
X	Quantity of PII	Provide explanation: A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.

X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, or the PII itself is likely to result in severe or catastrophic harm to the individual or organization
X	Obligation to Protect Confidentiality	Provide explanation: Organization or Mission- specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government- wide or industry-specific requirements. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization- owned equipment outside of the physical locations owned by the organization only with a secured connection
	Other:	Provide explanation

Section 12: Analysis

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

	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.

Enclosure

COMMERCE/CENSUS-8

SYSTEM NAME:
Statistical Administrative Records System.

SECURITY CLASSIFICATION:
None.

SYSTEM LOCATIONS:

Bowie Computer Center, Bureau of the Census, 17101 Melford Blvd., Bowie, Maryland 20715; and at a FEDRAMP-approved cloud services facility.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system covers the population of the United States and territories. In order to approximate coverage of the population in support of its statistical programs, the Census Bureau will acquire administrative record files from agencies such as the Departments of Agriculture, Education, Health and Human Services, Homeland Security, Housing and Urban Development, Labor, Treasury, Veterans Affairs, the Office of Personnel Management, the Social Security Administration, the Selective Service System, and the U.S. Postal Service. Comparable data may also be sought from state agencies and commercial sources and Web sites.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system of records are organized into three components:
•The first category contains records with personal identifiers (names and Social Security Numbers (SSNs)), with access restricted to a limited number of sworn Census Bureau staff. These records are only used for a brief period of time while the personal identifiers are replaced with unique non-identifying codes. In a controlled Information Technology (IT) environment, the identifying information (SSN) contained in source files is removed and replaced with unique non-identifying codes. The Census Bureau does not collect SSNs in Title 13 surveys or censuses. Title 13, Section 6, authorizes the Census Bureau to acquire information from other federal departments and agencies and for the acquisition of reports of other governmental or private sources. Data acquired by the Census Bureau to meet this directive may include direct identifiers such as name, address, date of birth, driver's license number, and SSN. The direct identifiers are used to identify duplicate lists and link across multiple sources.

•The Census Bureau has developed software to standardize and validate incoming person records to assign a unique Census Bureau linkage identifier. This identifier, called the Protected Identification Key (PIK), is retained on files so that SSNs can be removed. This process occurs through the Person Identification Validation System (PVS). The PVS software processes direct identifiers from input files. Census Bureau staff use the person linkage keys to merge files when conducting approved research and operations activities. The software is also used to facilitate record linkage for Census Bureau research partners within the Federal Statistical System. Through legal agreements, linkage keys may be created by the Census Bureau for other Federal Statistical Agencies to produce statistics. The PVS system does not append additional identifying information, only a unique identifier to facilitate record linkage.

•The second category contains records that are maintained on unique data sets that are extracted or combined on an as-needed basis in approved projects. Records are extracted or combined as needed using the unique non-identifying codes, not by name or SSN, to prepare numerous statistical products. These records may contain information such as: Demographic information—date of birth, sex, race, ethnicity, household and family characteristics, education, marital status, tribal affiliation, and veteran's status, etc.; Geographical information—address and geographic codes, etc.; Mortality information—cause of death and hospitalization information; Health information—type of provider, services provided, cost of services, and quality indicators, etc.; Economic information—housing characteristics, income, occupation, employment and unemployment information, health insurance coverage, Federal and State program participation, assets, and wealth.

•The third category contains two types of records that use name data for specific research activities. The Census Bureau has policies and procedures to review and control name data from administrative records providers and third party sources. This category refers to name data used to plan contact operations for surveys and censuses and for research on names. The first type of records includes Respondent contact information—name (or username), address, telephone number (both landline and cell phone number), and email address or equivalent. The second type of records includes name data used to set Demographic Characteristics Flags—names are compared to lookup tables and used in models to assign sex and ethnicity. Records in this category are maintained on unique data sets that are extracted or combined on an as-needed basis using the unique non-identifying codes that replaced the SSNs, but with some name information retained.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title 13 U.S.C. 6.

PURPOSES:

This system of records supports the Census Bureau's core mission of producing economic and demographic statistics. To accomplish this mission the Census Bureau is directed to acquire information from public and private sources to ensure the efficient and economical conduct of its censuses and surveys by using that information instead of conducting direct inquiries. To provide the information on which the American public, businesses, policymakers, and analysts rely, the Statistical Administrative Records System efficiently re-uses data from external sources, thereby eliminating the need to collect information again. Therefore, the purpose of this system is to centralize and control the use of personally identifiable information by providing a secure repository that supports statistical operations. The system removes SSNs contained in source files and replaces them with unique non-identifying codes called Protected Identification Keys (PIKs) prior to use by other Census Bureau operating units. Census Bureau staff use the PIK to merge files to conduct approved research projects. Through legal agreements documenting permitted uses of the external data, linked files may be created to produce statistics. By combining survey and census data with administrative record data from other agencies, and data procured from commercial sources, the Census Bureau will improve the quality and usefulness of its statistics and reduce the respondent burden associated with direct data collection efforts. The system will also be used to plan, evaluate, and enhance survey and census operations; improve questionnaire design and selected survey data products; and produce research and statistical products such as estimates of the demographic, social, and economic characteristics of the population.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

None. The Statistical Administrative Records System will be used only for statistical purposes. No disclosures which permit the identification of individual respondents, and no determinations affecting individual respondents will be made.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:
None.
POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records will be stored in a secure computerized system and on magnetic media; output data will be electronic. Magnetic media will be stored in a secure area within a locked drawer or cabinet. Source data sets containing personal identifiers will be maintained in a secure restricted-access IT environment. Records may also be stored by or at a secure FEDRAMP-approved cloud service provider or facility.

RETRIEVABILITY:

Staff producing statistical products will have access only to data sets from which SSNs have been deleted and replaced by unique non-identifying codes internal to the Census Bureau. Only a limited number of sworn Census Bureau staff, who work within a secure restricted-access environment, will be permitted to retrieve records containing direct identifiers (such as name or SSN).

SAFEGUARDS:

The Census Bureau is committed to respecting respondent privacy and protecting confidentiality. Through the Data Stewardship Program, we have implemented management, operational, and technical controls and practices to ensure high-level data protection to respondents of our censuses and surveys.

•An unauthorized browsing policy protects respondent information from casual or inappropriate use by any person with access to Title 13 protected data.

•All Census Bureau employees, persons with special sworn status, as well as employees of FEDRAMP-approved cloud services who may have incidental access to Title 13 protected data, are subject to the restrictions, penalties, and prohibitions of 13 U.S.C. 9 and 214 as modified by Title 18 U.S.C. 3551, et. seq.; the Privacy Act of 1974 (5 U.S.C. 552a(b)(4); 18 U.S.C. 1905; 26 U.S.C. 7213, 7213A, and 7431; and 42 U.S.C. 1306.

•All Census Bureau employees and persons with special sworn status will be regularly advised of regulations issued pursuant to Title 13 governing the confidentiality of the data, and will be required to complete an annual Data Stewardship Awareness training and those who have access to Federal Tax Information data will be regularly advised of regulations issued pursuant to Title 26 governing the confidentiality of the data, and will be required to complete an annual Title 26 awareness program. The restricted-access IT environment has been established to limit the number of Census Bureau staff with direct access to the personal identifiers in this system to protect the confidentiality of the data and to

prevent unauthorized use or access. These safeguards provide a level and scope of security that meet the level and scope of security established by OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources.

•All Census Bureau and FEDRAMP-approved computer systems that maintain sensitive information are in compliance with the Federal Information Security Management Act, which includes auditing and controls over access to restricted data.
•The use of unsecured telecommunications to transmit individually identifiable information is prohibited.

•Paper copies that contain sensitive information are stored in secure facilities in a locked drawer or file cabinet behind a closed door.

•Each requested use of the data covered in this SORN will be reviewed by an in-house Project Review Board to ensure that data relating to the project will be used only for authorized purposes. All uses of the data are solely for statistical purposes, which by definition means that uses will not directly affect benefits or enforcement actions for any individual. Only when the Project Review Board has approved a project, will access to information from one or more of the source data sets occur. Data from external sources in approved projects will not be made publicly available.

•Any publications based on the Statistical Administrative Records System will be cleared for release under the direction of the Census Bureau's Disclosure Review Board, which will confirm that all the required disclosure protection procedures have been implemented. No information will be released that identifies any individual.

RETENTION AND DISPOSAL:

Records are to be retained in accordance with General Records Schedule GRS 4.3, and the Census Bureau's records control schedule DAA-0029-2014-0005, Records of the Center for Administrative Records Research and Applications, which are approved by the National Archives and Records Administration (NARA). Records are also retained in accordance with agreements developed with sponsoring agencies or source entities. Federal tax information administrative record data will be retained and disposed of in accordance with Publication 1075, Tax information Security Guidelines for Federal, State, and Local Agencies and Entities. The Census Bureau issues an Annual Safeguard Security Report that includes information on the retention and disposal of federal tax information. Pursuant to IRS regulation, Title 26 U.S.C. 6103(p)(4)(F)(ii), data cannot be transferred to NARA.

SYSTEM MANAGER(S) AND ADDRESS:

Associate Director for Research and Methodology, U.S. Census Bureau, 4600 Silver Hill Road, Washington, DC 20233-8000.

NOTIFICATION PROCEDURE:

None.

RECORD ACCESS PROCEDURES:

None.

CONTESTING RECORD PROCEDURES:

None.

RECORD SOURCE CATEGORIES:

Individuals and addresses covered by selected administrative record systems and Census Bureau censuses and surveys including current demographic and economic surveys, quinquennial Economic Censuses, and decennial Censuses of Population and Housing. Additionally, the Census Bureau will also acquire administrative record files from agencies such as the Departments of Agriculture, Education, Health and Human Services, Homeland Security, Housing and Urban Development, Labor, Treasury, Veterans Affairs, the Office of Personnel Management, the Social Security Administration, the Selective Service System, and the U.S. Postal Service, etc. Comparable data may also be sought from state agencies, commercial sources, and Web sites.

SYSTEM EXEMPTIONS FROM CERTAIN PROVISIONS OF THE ACT:

Pursuant to 5 U.S.C. 552a(k)(4), this system of records is exempted from the notification, access, and contest requirements of the agency procedures (under 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f)). This exemption is applicable as the data are maintained by the Census Bureau solely as statistical records, as required under Title 13, and are not used in whole or in part in making any determination about an identifiable individual. This exemption is made in accordance with the Department's rules which appear in 15 CFR part 4 Subpart B published in this Federal Register.

FEDERAL REGISTER HISTORY:

81 FR 76554 November 13, 2016 Notice of Proposed Amendment to Privacy Act System of Records
75 FR 78211 December 15, 2010 Effective Date Notice
75 FR 66061 October 27, 2010 Notice of Proposed Amendment to Privacy Act System of Records