

Exhibit 5

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



Privacy Impact Assessment
for the
CEN05 Field Systems Major Application System
March 2018

Reviewed by:


Robin J. Bachman

, 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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the
Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.06.22 13:49:29 -04'00'

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

Date

**U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/CEN05 Field Systems Major Application System**

Unique Project Identifier: 006-000401400

Introduction: System Description

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

- (a) The CEN05 Field Systems Major Application System is a major information system managed by the Application Development Services Division (ADSD) in support of the Census Bureau Field Directorate.
- (b) The IT system is housed at the Census Bureau's Bowie, MD computer center.
- (c) CEN05 interconnects with other CENs. Desktop and laptop client services are provided by CEN17, server support is provided by CEN16, and Oracle 12c database support is provided by CEN18.
- (d) How the system operates to achieve the purpose(s) identified in section 4:

The Field Directorate plans, organizes, coordinates, and carries out the Census Bureau's field data collection program for sample surveys, special censuses, the Economic Census, and the Decennial census. The CEN05 IT system maintains Personally Identifiable Information (PII) collected from respondents for these surveys and censuses such as name, address, contact information, race, gender, education, financial information, etc. In addition, Field Representative characteristics are also collected while surveys and census interviews are conducted.

Laptops are used to collect survey data in the field. An application assigns cases and monitors interviewing progress. Information systems covered by other CEN plans are used as routing mechanisms to transfer survey data from various survey sources, that includes but are not limited to, computer interviewing, telephone interviewing utilizing Census computer programs, internet self surveys, and paper surveys to the survey sponsors.

In addition to laptops, the Field Directorate has begun utilizing both tablet and other mobile computing devices to perform Census Tests that lead up to the 2020 Decennial Census to collect respondent information using Census Bureau issued mobile devices.

The Customer Experience Management (CEM) System is a centralized data store from five data sources currently being utilized by the Census Bureau and will deploy an enterprise dashboard for Census Bureau leadership.

This dashboard will provide insights into customer engagement for Census Bureau products & services, and will allow analysts to leverage data across data sources on a

holistic Business Intelligence (BI) platform. The system will not only eliminate manual processes but will:

- 1) Create an opportunity for a better understanding of patterns and trends of customer experiences that can lead to actionable improvement plans, and;
- 2) Establish a framework and foundation for other data integration, BI, and analytics efforts.

CEM will interface/collect information for various sources inside and outside of the Census Bureau and will contain PII data.

The Census Enterprise Data Collection and Processing initiative (CEDCaP) is a suite of systems and supporting infrastructure to handle data collection and processing for the nearly 100 surveys and three censuses conducted by the Census Bureau. CEN05 is part of this infrastructure and includes the *Enterprise Censuses and Surveys Enabling platform (ECaSE)* which will provide about half the data collection capabilities for CEDCaP

The ECaSE – ISR (Internet Self-Response) secure Internet data exchange system is a web-based framework for the design, delivery, and execution of surveys, censuses, and other data collection and data exchange efforts over the Internet. The enterprise-level application offers data collection areas the ability to reach a large number of potential respondents online, in a customizable manner to suit their business needs. ECaSE – ISR is developed to support increased demand for online data collections, including the extremely high loads associated with the 2020 Decennial Census.

ECaSE – OCS (Operational Control System) will serve as the standard tool to assign, control, track, and manage listing, survey and census workloads for the field workforce. ECaSE – OCS provides an enterprise application framework for this need, regardless of the interviewer-assisted mode used (phone or in person).

To establish a cohesive system boundary for the purposes of security assessment, the CEN05 IT system is comprised of three major areas: Collections, Business Support Processes, and Backend Processes. Each of these major components employs security control mechanisms that must be individually documented to ensure that the system as a whole is appropriately protected. As such, the system security plan is organized to reflect the implementation of technical controls for each subsystem component.

ADSD incorporated a Survey Field Identification Tool (sFIT) to aid in investigating situations where it is suspected that a Field Representative may be falsifying respondent information. The tool will be used by Contact Center and Regional Office (RO) representatives to indicate FR who are suspected of falsification and to facilitate and document the results of the investigations. The newly developed tool replaced the previous automated system and the paper 11-163 forms. sFIT collects and disseminates PII regarding a survey respondent and the Field Representative who is suspected of falsifying survey data. sFIT received its Authority to Operate (ATO) on 7/13/2017.

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

There are many external sponsors but CEN05 does not have direct connections to any of them. Demographics Survey Division (DSD), Econ, etc., will give CEN05 the surveys that they have crafted for the external sponsors and the data collected for those surveys is placed into the CEN05 Master Control System (MCS) for the internal system to pick up. It will be the other internal sponsors' responsibility to vet the information, transform it into a format that the external sponsors can ingest and send it off. The sharing of the data should be on those systems with the external connection to the external sponsors. This is the same with the National Center for Health Statistics (NCHS) survey.

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

The CEN05 IT system includes a data warehouse that extracts and provides a view of survey data over time, data collection modes, and data collection operations. It aggregates data and creates canned reports. These reports are made available to stakeholders, approved individuals, and organizations to support optimization and coordination of decennial, current, and special surveys. The reports are developed by a special staff that was established through the Office of the Director to serve as an analytic team with specific, ongoing, responsibilities to develop analytic tools (charts and tables). These tools will be used by decennial and current survey field managers toward the goal of continuous improvement in survey operational efficiency. This group will both initiate and respond to issues related to survey performance indicators including cost, data quality, and data collection progress. This database interfaces with systems throughout the Census Bureau that contain PII, Business Identifiable Information (BII), and data collected and/or protected under Title 13 and Title 26.

(g) Any information sharing conducted by the system

The CEN05 IT system only shares PII and BII data within other CEN05 systems/components and with other Census Bureau IT systems. The data warehouse provides the ability for survey sponsors to view statistical data. It does not allow access to the information at the individual case level where the "raw" data resides. The data warehouse interacts with multiple systems within the Census Bureau network such as the system that contains information about businesses, which provides the mailing list for the Economic Census, and the primary sampling frame for virtually all other business surveys. The survey information about businesses is collected to track the movement of commodities from businesses throughout the United States. The data will be stored in its "raw" form and then transformed and stored in the data warehouse. The data warehouse will tabulate the data and display it in various reports. The data in its "raw" form will not be displayed. The data warehouse maintains PII, BII, Title 13 and Title 26 information.

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

15 U.S.C. 301.
 13 U.S.C. Chapter 5, 6(c), 8(b), 131, 132, 141, 161, 182, 193, 196
 18 U.S.C. 2510-2521
 15 CFR, Part 50.
 26 U.S.C.

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

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

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

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

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

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

- 1) Employee's full SSN info needed for cost reimbursement and other financial purposes.
- 2) The last 4 digits of the survey respondent's SSN helps is collected on behalf of the survey sponsor, The National Center for Health Statistics (NCHS). 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 Social Security Number (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 Social Security Number 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	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	XX

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	XX
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	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X

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	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	X	Commercial Data Brokers	X
Third Party Website or Application					

Other (specify):

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

It will be the internal sponsors' responsibility to vet the information, transform it into a format that the external sponsors can ingest and send it off. The sharing of the data should be on those systems with the external connection to the external sponsors.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

- 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):			
	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

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).

Census Bureau information shapes important policy and operational decisions that help improve the nation's social and economic conditions. We conduct the constitutionally mandated Census of Population and Housing every 10 years, which is used to apportion seats in the House of Representatives and informs congressional redistricting.

We also conduct a census of all business establishments and of all governmental units, known respectively as the Economic Census and the Census of Governments, every five years. The Economic Census is the benchmark used for measuring Gross Domestic Product (GDP) and other key indicators that guide public policy and business investment decisions.

In addition, we conduct several ongoing business and household surveys that provide the information in several of the Nation's key economic indicators and which is used to allocate over \$400 billion in Federal funding annually.

The PII/BII collected for statistical purposes: The PII/BII maintained is from voluntary and mandatory surveys, census interviews, pilot tests and cognitive interviews collected from members of the public.

The PII collected for administrative purposes: We collect information about Census Bureau employees during the collection of respondent information. Field representative and interviewer characteristics obtained during census and survey interviews, pilot tests, and cognitive interviews are used for research and analytical studies to evaluate Census Bureau surveys and programs.

- 5.2 Describe any potential threats to privacy 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 Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census 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 Data Loss Prevention solution as well.

All 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.

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			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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

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

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
---	---

CEN03, CEN04 CBS, CEN06 NPC, CEN11, CEN13, CEN22, CEN35, CEN36
CEN05 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 the 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):			

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:	
X	Yes, notice is provided by other means.	Specify how: as specified in some survey instrument(s), respondent letters, etc.
	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: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For mandatory surveys or censuses, the respondent does not have an opportunity to decline to provide PII/BII

- 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: For Employee Productivity Measurement Records the consent is required for employment
X	No, individuals do not have an opportunity to consent to particular	Specify why not: As identified in the applicable SORNs Census -3, -4, -5, and -7 the records are exempted from

	uses of their PII/BII.	notification, access, and contest requirements of the agency procedures (under via 5 U.S.C 552a(c)(3),(d), (e),(1), (e),(4),(G), (H) and (I), and (f). The data are maintained by the U.S. Census Bureau solely as statistical records as required under Title 13 U.S.C., and are not used in whole or in part in making any determination about an identifiable individual. This exemption is also made in accordance with the Department's rules which appear in 15 CFR part 4 subpart B.
--	------------------------	---

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: : As identified in the applicable SORN for Employee Productivity Measurement Records, these individual may contact the Associate Director for Field Operations for access to these records.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: As identified in the applicable SORNs Census-3, -4, -5, and -7 the records are exempted from notification, access, and contest requirements of the agency procedures (under via 5 U.S.C 552a(c)(3),(d), (e),(1), (e),(4),(G), (H) and (I), and (f). The data are maintained by the U.S. Census Bureau solely as statistical records as required under Title 13 U.S.C., and are not used in whole or in part in making any determination about an identifiable individual. This exemption is also made in accordance with the Department's rules which appear in 15 CFR part 4 subpart B.

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:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>7/20/2017</u> ☐ 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 supporting 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 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 Review 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).*

The Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census 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 Data Loss Prevention 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, number, and link. <i>(list all that apply):</i> COMMERCE/CENSUS-2, Employee Productivity Measurement Records: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-2.html COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html COMMERCE/CENSUS-4, Economic Survey Collection: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5, Decennial Census Program:
---	---

	http://www.osec.doc.gov/opog/PrivacyAct/SORNS/census-5.html
	COMMERCE/CENSUS-7, Special Censuses of Population Conducted for State and Local Government: http://www.osec.doc.gov/opog/PrivacyAct/SORNS/census-.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: GRS 3.1: General Technology Management Records; GRS 3.2: Information Systems Security Records; GRS 4.1: Records Management Records; GRS 4.2: Information Access and Protection Records; GRS 4.3: Input Records, Output Records, and Electronic Copies, N1-29-89-5 American Housing Survey, NC1-29-79-7 Demographic Fields Area, NC1-29-80-6 Demographic and Economic area Divisions - Secondary Use Sampling Records
	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		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 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 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 PII 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. PII in this IT system is collected under the authority of Title 5.
X	Access to and Location of PII	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 (e.g., virtual private network (VPN)).
	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.)

The biggest potential threat to privacy is the potential loss of a Field Representative's CAPI laptop. This threat is mitigated by the use of full disk encryption of the hard drive or solid state drive which renders the data inaccessible in the event that laptop is lost, damaged, or stolen.

Due to the quantity, nature, and scope of the multiple surveys collected and processed through CEN05 (including the upcoming Decennial Census), there are no plans to reduce the quantity or type of data being collected, nor the sources of that data.

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.

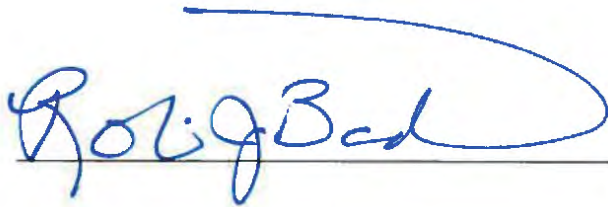
	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Exhibit 6

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



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

Reviewed by: , Bureau Chief Privacy Officer

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the
Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.09.28 19:04:38 -04'00'

09/27/2018

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

Date

**U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/CEN08 DITD**

Unique Project Identifier: 006-000400400

Introduction: System Description

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

The response must be written in plain language and be as comprehensive as necessary to describe the system. Please answer each question (a) through (i) separately.

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

CEN08 Decennial Information Technology Division (DITD) consists of both general support systems and major applications:

Major Applications

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

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

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

General Support System

CEN08 DITD general support system consists of:

- 1) an external vendor general support system called the Third Party Fingerprinting solution that is managed by Indrasoft. The U.S. Census Bureau (USCB) employs hundreds of thousands of temporary workers to perform data collection activities via a non-competitive Schedule A hiring authority from the Office of Personnel Management (OPM) in support of the Decennial Census testing in Fiscal Year (FY) 2018 and 2020 Census. As part of the recruitment and security process, the USCB requires that these selectees undergo fingerprinting to determine their suitability for employment. In addition, contractors that provide services in support of the 2020 Decennial Census, such as Census Questionnaire Assistance (CQA) contractor candidates, may also be

fingerprinted. To support fingerprinting for the 2020 Census, the USCB will use the Third Party Fingerprinting solution to capture and transmit fingerprints to USCB and conduct identity proofing for these temporary hires and contractors.

- 2) CEN08 DITD also consists of another external vendor general support IT system called the Recruiting and Assessment (R&A) solution that is managed by Cornerstone OnDemand. R&A is a FedRAMP-approved IT system that allows the Census Bureau to have a recruiting & selection tool and a learning management tool in one. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

(b) System location

Decennial Applications – Bowie Computer Center (BCC) and AWS GovCloud located in Oregon.

Third Party Fingerprinting – AWS U.S. East/West located in US East (Ohio), US East (N. Virginia), US West (N. California), and US West (Oregon) and physical fingerprinting capture sites across the United States.

R&A - Unified Talent Management Suite (CUTMS) Cloud located in El Segundo, CA and Ashburn, VA.

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

Decennial Applications – Shares information internally within the Census Bureau with CEN07 GEO, CEN05 Field, CEN11 DEMO, CEN18 CDL, CEN19 CEDSCI, CEN21 DAPPS, CEN30 ACS, and CEN36 ADEP.

Third Party Fingerprinting – Shares information internally within the Census Bureau with CEN21 CHEC and CEN18 SOA.

R&A – Shares information internally within the Census Bureau with *CEN21 DAPPS*

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

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

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

Temporary hires and contractors looking to support the 2020 Census submit their job applications through the R&A system. R&A securely delivers the submitted application data and associated attachments to DAPPS for processing and selecting.

To support fingerprinting for the 2020 Census, the USCB will use the Third Party Fingerprinting solution to capture and transmit fingerprints to USCB and conduct identity proofing for temporary hires and contractors (selectees). These selectees will provide their fingerprints at one of the Third Party Fingerprinting physical capture sites.

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

Information in the CEN08 DITD systems are retrieved by using PII information identified in Section 2 below by authorized users using internal web applications, secure databases, and managed file transfer servers. Authorized Census Hiring Employment Check (CHEC) users pull selectee fingerprint files from the Third Party Fingerprinting solution and forward to the FBI for processing.

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

Information is transferred to and from CEN08 DITD systems via authorized manual and/or automated connections.

User fingerprints are captured on Third Party Fingerprinting physical sites which is uploaded to authorized AWS U.S. East/West. Files are encrypted and transferred using the service-oriented architecture (SOA) via the Enterprise Service Bus (ESB), which then sends it over to CHEC within the U.S Census Bureau. The Enterprise Service Bus is a configuration-based, policy-driven enterprise service bus. It provides highly scalable and reliable service-oriented integration, service management, and traditional message brokering across heterogeneous IT environments. It combines intelligent message brokering with routing and transformation of messages, along with service monitoring and administration in a unified software product.

(g) Any information sharing conducted by the system

CEN08 DITD systems share information internally with approved Census Bureau systems on an as needed basis.

Fingerprints are shared between the fingerprinting solution, CHEC and FBI.

R&A Applicant information is shared internally with the Decennial Applicant, Personnel and Payroll System (DAPPS).

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

Title 13, U.S.C. Section 6c

Title 13, U.S.C. Section 141

Title 13, U.S.C. Section 193

44 U.S.C. Section 3101

41 U.S.C. 433(d)

5 U.S.C. 301

5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397

Executive Order 12107

Executive Order 12564

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

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

 x 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): New Third Party Fingerprinting solution.					

_____ 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.

Section 2: Information in the System

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

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

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

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

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

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

Other Information (specify)					

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

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

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

Non-government Sources					
Public Organizations		Private Sector	x	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.

CEN08 DITD 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 data validation controls to ensure accuracy of information.

Selectee information is verified for accuracy when individuals schedule their fingerprints by verification against other forms of identification. Further, background checks are performed by the FBI to validate name, credit, and criminal history.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
x	No, the information is not covered by the Paperwork Reduction Act.

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	x
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

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

Section 3: System Supported Activities

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

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

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

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	x
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	x
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For Statistical Purposes (i.e. Censuses/Surveys)			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The PII collected, maintained, and/or disseminated by the CEN08 IT system is in reference to members of the public. Data collection is used to produce national statistical information.

Third Party Fingerprinting is capturing selectee fingerprint data on behalf of the U.S Census Bureau to hire selectees to help conduct the 2020 Census operations. The third party vendor is mandated to only utilize FedRAMP authorized solutions. The vendor does not directly submit the fingerprint information to the FBI, rather the information is securely sent to the U.S Census Bureau for processing and submission to the FBI.

- 5.2 Describe any potential threats to privacy 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.)

CEN08 DITD systems adhere to the Information Technology Security Program Policy as it relates to handling, retaining, and disposing collected information. Census Bureau information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention (DLP) solution as well.

Fingerprints are retained for 120 days and then disposed of following NIST sanitation guidance. All individuals that handle PII are required to complete annual Data Stewardship Awareness training.

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			
Federal agencies		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 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: Decennial Applications – Shares information internally within the Census Bureau with CEN07 GEO, CEN05 Field, CEN11 DEMO, CEN18 CDL, CEN19 CEDSCI, CEN21 DAPPS, CEN30 ACS, and CEN36 ADEP. Third Party Fingerprinting – Shares information internally within the Census Bureau with CEN21 CHEC and CEN18 SOA. R&A – Shares information internally within the Census Bureau with CEN21 DAPPS CEN08 uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users

General Public		Government Employees	x
Contractors	x		
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.census.gov/about/policies/privacy/privacy-policy.html	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

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

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Employment with the U.S. Census Bureau is voluntary.
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: According to Title 13, Section 221 (Census, Refusal or neglect to answer questions; false answers) of the United States Code, persons who fail or refuse to respond to the mail-back census form, or refuse to respond to a follow-up Census Bureau taker can be fined up to \$100. Persons who knowingly provide false information to the Census Bureau can be fined up to \$500. For Census Bureau employees who access systems in CEN08 providing PII is a requirement for employment.

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

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Employment with the U.S. Census Bureau is voluntary. Temporary hires and contractors have to consent to the U.S. Census Bureau uses of their PII.
x	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For records covered by SORN Census-5, Decennial Census Programs, there are no access and consent requirements since the data is collected for statistical purposes only. For Census Bureau employees consent to particular uses of PII is a requirement for employment.

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

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Selectee information is verified for accuracy when individuals schedule their fingerprints.
x	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For records covered by SORN Census-5, Decennial Census Programs, there is no opportunity to review/update data unless the Census Bureau contacts the respondent for an update on their information. For Census Employees, employees have access to PII via the appropriate Human Resources applications that reside outside of the CEN08 IT system.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition to IT system processes that handle PII, all manual extractions for PII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>July 25, 2018</u> [] 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 supporting 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 ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

Census Bureau information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well.

Section 9: Privacy Act

- 9.1 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. <i>(list all that apply):</i> COMMERCE/CENSUS-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/DEPT-13, Investigative & Security Records- http://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-13.html COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html OPM SORN GOVT-5, Recruiting, Examining and Placement Records- https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-5-recruiting-examining-and-placement-records.pdf
	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: N1-29-05-01, N1-29-10-5, GRS 3.1, GRS 5.6 item 181
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

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

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

- 11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same 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 levels. *(Check all that apply.)*

X	Identifiability	PII collected can be directly and indirectly used to identify individuals.
X	Quantity of PII	The collection is for the decennial census, therefore, a severe or substantial number of individuals would be affected if there was loss, theft or compromise of the data. This could affect decennial 2020 Census response rates and have a long term effect on the Nation's population count. Severe collective harm to the USCB's

		reputation, or cost to the USCB in addressing a breach.
X	Data Field Sensitivity	The PII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
X	Context of Use	Disclosure of PII in this IT system or the PII itself may result in severe harm to the individual or organization.
X	Obligation to Protect Confidentiality	PII collected is required to be protected in accordance with 5, U.S.C (552a) and 13, U.S.C, section 9.
X	Access to and Location of PII	The PII is located on computers (including laptops) and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know including the Census Bureau regional offices and survey program offices, etc. Access is allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities. PII is also located on U.S. Census Bureau authorized vendor systems. Access is limited to those with a need-to-know for authorized U.S. Census Bureau contractors and employees.
	Other:	Provide explanation:

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.)

A third party vendor is capturing selectee fingerprint data and PII on behalf of the U.S Census Bureau. The third party vendor is mandated to only utilize authorized systems and FedRAMP solutions. The vendor does not directly submit the fingerprint information to the FBI, rather the information is securely sent to the U.S Census Bureau for processing and submission to the FBI.

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.

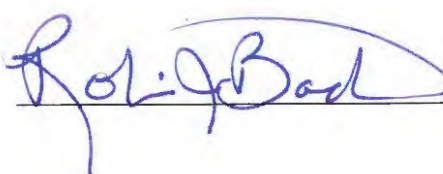
	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.

Exhibit 7

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



**Privacy Impact Assessment
for the
CEN11 Demographic Census, Surveys, and Special Processing**

Reviewed by:  4/17/18, 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

CATRINA PURVIS

 Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the
Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.06.22 13:55:40 -04'00'

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

Date

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

Unique Project Identifier: 006-000400500

Introduction: System Description

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

The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

The U.S. Census Bureau's CEN11 Demographic Census, Surveys, and Special Processing System is a system comprised of components that support the Demographic Directorate business functions. The component within CEN11 that contains PII is a Commercial off the Shelf (COTS) product used by Census Bureau demographic programs for data access, transformation, reporting, and statistical analysis. Some of the demographic data maintained in this system are Name, date of birth, telephone number, occupation, military service information (if applicable), medical information, financial information etc.

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

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

- Face-to-face or telephone induction interviews
- Field Representatives (FR)
- Web-based respondents

The information is collected by using:

Web-based respondents use a web-based application instrument that resides on the Census Bureau network via CEN15 Centurion. Respondents use their personal computers to access Centurion.

Introduction interviews are collected using electronic instruments – Computer-Assisted Personal Interviewing (CAPI) (a CEN05 component).

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

(c) any information sharing conducted by the system

There is PII being shared as follows:

- The Census Bureau provides access to staff at Department of Housing and Urban

Development (HUD) with Special Sworn Status (SSS) for the American Housing Survey (AHS) via the Census Bureau Virtual Desktop Infrastructure (VDI).

- The Census Bureau provides some Bureau of Labor Statistics (BLS) Staff access to Current Population Survey (CPS) and Consumer Expenditure Survey (CES) data on a CEN11 Server in the DMZ. BLS Staff have Special Sworn Status (SSS) to have Census accounts to access the server. Consumer Expenditure staff at BLS access CPS data for weighting purposes.
- Census Bureau sends a file containing respondent addresses to BLS for the Telephone Point of Purchase Survey (TPOPS).
- The Census Bureau sends data files to the National Center for Health Statistics (NCHS) for the National Ambulatory Medical Care Survey (NAMCS), the National Hospital Ambulatory Medical Care Survey (N(H)AMCS) and National Health Interview Survey (NHIS). Data transfers are conducted through the Centers for Disease Control and Prevention (CDC) Secure Access Management Services (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 Schools and Staffing Survey (SSS), the Private School Survey (PSS), the National Teacher and Principal Survey (NTPS), the Teacher Follow-up Survey (TFS), the Principal Follow-Up Survey (PFS) and the Beginning Teacher Longitudinal Survey (BTLS). Data transfers are conducted through the Institute of Education Sciences (IES) Members Site.

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

13 USC sections 8(b), 182 and 18 U.S.C. 2510-2521

(e) the Federal Information Processing Standard (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 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		i. Credit Card	
b. Taxpayer ID	x	f. Driver's License		j. Financial Account	
c. Employer ID	x	g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: The last 4-digits of the SSN is used in admin records matching to the National Health Interview Survey (NHIS). The justification for the necessity of collecting this information, taken from the latest approved OMB ICR supporting statement is below: Social Security Number and Health Insurance Claim Number: The last four digits of the Social Security Number (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 Social Security Number 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	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	x
f. Race/Ethnicity	x	l. Education	x	r. Mother's Maiden Name	
s. Other general personal data (specify): Citizenship					

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			
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	x	f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address		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	x	Online	x
Telephone	x	Email	x		
Other (specify):					

--

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

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

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

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

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

Section 3: System Supported Activities

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

Activities			
Audio recordings	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 Survey of Income and Program Participation (SIPP); future plans are to incorporate CARI for all 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			
To determine eligibility		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For statistical purposes (i.e., Censuses/Surveys)			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII is used to process numerous national statistical surveys and other demographic data programs.

The data is used to calculate, process, and manipulate 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 information that is collected in this system is from members of the public.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x	x	x

DOC bureaus			
Federal agencies		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 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: CEN11 shares information with CEN03, CEN07, CEN08, CEN13, CEN14, CEN18, CEN19, and CEN30. CEN11 receives information from CEN13, CEN30, and CEN35. The CEN11 IT 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 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):			

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: CEN11 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 SORNs 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.

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 is 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:
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>7/14/2017</u> ☐ 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	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): Publications are approved by the Disclosure Review 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 limited to the following:

- Intrusion Detection / Prevention Systems (IDA/IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards, including special publications 800-53, 800-63, 800-37 etc. Any system within the Census that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implanted and operating as intended. Census also deploys a DLP solution as well.

Section 9: Privacy Act

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

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

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> :
x	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> . 1. Census -3, Demographic Survey Collection (Census Bureau Sampling Frame) submitted on 7/22/16. 2. Census-7, Demographic Survey Collection (non-Census Bureau Sampling Frame) submitted on 7/22/16.
	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: N1-29-99-5, N1-29-89-3, N1-29-87-3, N1-29-86-3, NC1-29-85-1, NC1-29-79-7, and GRS 3.1 GRS 3.2 GRS 4.1, GRS 4.3
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	x	Overwriting	x
Degaussing		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: PII/BII 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/BII, 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/BII in this IT system or the PII/BII itself may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with 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	PII/BII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access is 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

I2.1 Indicate whether the conduct of this PIA results in any required business process changes.

x	Yes, the conduct of this PIA results in required business process changes. Explanation: Next PTA will be update selection in question 2 to yes to address audio recordings and consistency with section 3.1 of the PIA.
	No, the conduct of this PIA does not result in any required business process changes.

I2.2 Indicate whether the conduct of this PIA results in any required technology changes.

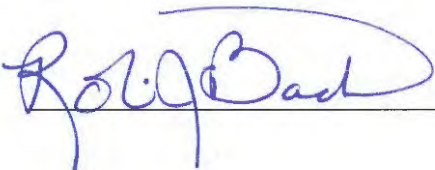
	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.

Exhibit 8

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



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

Reviewed by:  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.I 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 addition to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 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 <i>(list all that apply)</i> : Census-8, Statistical Administrative Records System
X	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> . 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.

Exhibit 9

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



Privacy Impact Assessment
for the
CEN18 Enterprise Applications

Reviewed by:

[Handwritten 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 14:19:48 -04'00'

Dr. Catrina D. Purvis

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

Date

U.S. Department of Commerce Privacy Impact Assessment U.S. Census Bureau CEN18 Enterprise Applications

Unique Project Identifier: 006-000401700

Introduction: System Description

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

The CEN18 Enterprise Applications system is the functional management framework used to deliver applications to end users of the U.S. Census Bureau network. The CEN18 Enterprise Applications system includes several applications that maintain or collect personally identifiable information (PII). These applications are:

- an enterprise-level data tracking system;
- a general support system for internal data management,
- a transaction-based system
- a relational database management system, and
- a concurrent analysis and estimation system (CAES),

Some examples of survey and census information maintained by this system are personal names, personal addresses, personal contact information (telephone numbers, email address), business information, occupation, medical information, tax information, etc. The systems reside in Census Bureau's Bowie Computing center. The components that collect PII/BII do not reside in the cloud.

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

The purpose of the enterprise-level data tracking system is to ensure data consistency, data integrity, and generate meaningful data information through data management, tracking, and reporting for Census Bureau collections.

The general support system for CEN18 provides internal data management within the Census Bureau collections. This system allows users to request access to datasets, and when approved, users are granted access to the datasets within a secure environment provisioned by the system. Census Bureau datasets are for internal use by employees, and are capable of containing protected or administrative information.

The transaction-based system within CEN18 serves as the primary mechanism for operational control across surveys for data collection. The system can be considered an operational brain that determines operational workflow based on pre-existing protocols.

The relational database management system stores and retrieves data as requested by other software applications. This system provides both a testing, development and production environment for optimum functionality.

The CAES serves as the enterprise-wide analytics platform for surveys and censuses. This system allows statisticians within census and survey projects to perform statistical models using census and survey response data, paradata, administrative records, and many other types of data. The system will receive PII including Identifying Numbers, General Personal Data, and Work-Related Data. The PII is received from other information systems that collect, maintain and disseminate Census and Survey data.

(c) any information sharing conducted by the system

The enterprise-level data tracking system does not share information.

The general support system shares information within the Census Bureau by querying indexed metadata and by sending email to data owners, administrators, and other application users.

The relational database management system does not share information.

The transaction-based system shares demographic survey, Decennial, and Economic Census information within the Census Bureau and with the Department of Commerce, that is used to determine new survey content, support electronic collections, for statistical purposes, and to create datasets for the Census Bureau.

The Concurrent Analysis and Estimation System (CAES) is an environment for use by researchers to make decisions during the data collection phase of a survey or a Census. The CAES system will provide the researcher with any data that they request as input and will output and send decision based data only to other systems. This could include things such as case level intervention codes, a stop work decision, or best time of day to contact respondents. CAES does not provide a mechanism for sharing PII/BII with other systems.

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

The legal authorities to collect PII and/or BII for CEN18 are:

5 U.S.C. 301

13 U.S.C. Chapter 9, and Sections: 6, 8(b), 9, 131, 132, 141, 161, 182, 193, 196

15 C.F.R. Part 30 and 19 C.F.R. Section 24.53

18 U.S.C. 2510-2521

26 U.S.C. 6103(j) and

Foreign Trade Statistical Regulations or its successor document, the Foreign Trade Regulations

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

The Federal Information Processing Standard (FIPS) 199 category for this system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

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

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

 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*		c. File/Case ID		i. Credit Card	X
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		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	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	X
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	X
s. Other general personal data (specify):					

Work-Related Data (WRD)

Version Number: 01-2015

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	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
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		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

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

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

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

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

☒	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):			

☒	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	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For research 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, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The PII/BII maintained for administrative purposes: This IT system maintains first name, last name, address, email address, etc. to ensure that mandatory survey or statistical, information is ready for internal Census use. The information pertains and is in reference to federal employees/contractors conducting the surveys and the public.

The PII/BII maintained for statistical and research purposes: The data maintained by this IT system is collected from other IT systems that collect censuses and surveys (e.g., responses and statuses) and is used to direct data collection efforts. It is also used to inform program areas within the Census Bureau (responsible for survey and census questionnaire mail out) whom to send survey and census forms to. The IT system gathers response data from the data collection modes to send it to the survey and census processing IT systems in a standardized way. This information enables the Census Bureau to fulfill its legal obligation to provide mandated statistics. The information pertains to members of the public.

The PII/BII maintained for information sharing initiatives: This information is collected and shared within the Census Bureau and the Department of Commerce to create datasets for various types of censuses and surveys. This information enables the Census Bureau to fulfill its legal obligation to enhance its information sharing initiatives. The information pertains to members of the public.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus	X		
Federal agencies			
State, local, tribal gov't agencies			

Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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

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

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: CEN01, CEN03, CEN04, CEN05, CEN07, CEN08, CEN10, CEN11, CEN13, CEN16, CEN17, CEN24, CEN26, CEN33 The CEN18 IT 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 the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public	☐	Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (Check all that apply.)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: 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.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to decline to provide PII/BII at the CEN18 system level.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
x	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to consent to particular uses of PII/BII at the CEN18 system level.

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: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to review/update PII/BII at the CEN18 system level.

Section 8: Administrative and Technological Controls8.1 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, audit logs are in place and assessed per NIST control AU-03, <i>Content of Audit records</i> .
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 20, 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.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. 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 <i>(list all that apply)</i>: COMMERCE/CENSUS-2, Employee Productivity Measurement Records: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-2.html COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html CENSUS-4, Economic Survey Collection:
---	---

http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5, Decennial Census Program: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/CENSUS-7, Special Censuses of Population Conducted for State and Local Government: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html COMMERCE/CENSUS-8, Statistical Administration Records Systems: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-8.html COMMERCE/CENSUS-9, Longitudinal Employer Household Dynamics System http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-9.html COMMERCE/CENSUS-12, Foreign Trade Statistics: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-12.html
Yes, a SORN has been submitted to the Department for approval on (date).
No, a SORN is not being created.

Section 10: Retention of Information

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

x	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1 GRS 3.2 GRS 4.1, GRS 4.2, GRS 4.3 Demographic Directorate NI-29-99-5, NI-29-89-3, NI-29-87-3, NI-29-86-3, NC1-29-85-1, NC1-29-79-7 Economics Directorate NI-029-10-2, NI-029-10-3, NI-029-12-004, NI-029-10-4 Company Statistics Division NI-29-10-1 Economic Surveys Division NI-29-03-1 NC1-29-80-15, NC1-29-79-4, NC1-29-78-15 NC1-29-78-8 Manufacturing and Construction Division NC1-29-81-10 Decennial Directorate NI-29-05-01, NI-29-10-5 American Community Survey DAA-0029-2015-0001
	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:
	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		Overwriting	
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: PII/BII collected can be directly used to identify individuals
X	Quantity of PII	Provide explanation: The collection is for demographic, Economic Surveys, and other surveys, and 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/BII, 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/BII in this IT system or the PII/BII itself may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance Title 13 collections. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	PII/BII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access is 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.
X	Identifiability	Provide explanation: PII/BII collected can be directly used to identify individuals

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.

Exhibit 10

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF COMMERCE,
et al.,

Defendants.

Civ. Action No. 18-2711

DECLARATION OF CHRISTOPHER WOLF

I, Christopher Wolf, declare as follows:

1. My name is Christopher Wolf. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I reside in Washington, DC, United States of America.
3. I am Senior Counsel in a Washington, DC law firm, focusing on privacy law.
4. The Electronic Privacy Information Center ("EPIC") is a non-profit, public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight of government activities that impact individual privacy, free expression, and democratic values. EPIC has a particular interest in preserving legal privacy protections for personal data, including the obligation of federal agencies to conduct privacy impact assessments.
5. I am a member of EPIC. EPIC's members are distinguished experts in law, technology, and public policy. As a member of EPIC, I serve on the EPIC Advisory Board, participate

in the activities of EPIC, help finance the activities of EPIC, and provide leadership for EPIC. I also pay annual membership dues, as required by the amended EPIC bylaws.

6. I became an EPIC Member because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age. As privacy lawyer, EPIC's work on these issues is of special importance to me.
7. EPIC works on my behalf to protect my privacy rights, and I rely on EPIC to obtain and disseminate information about government activities that threaten my privacy.
8. As a resident of the United States, I understand that the Census Bureau intends to ask for my citizenship status on the 2020 Census. By law, I am required to provide a truthful response to such a question.
9. The Census Bureau has indicated that it may disclose my citizenship status to other federal agencies, including for criminal law enforcement purposes.
10. The imminent collection and possible disclosure of my citizenship status by means of the 2020 Census is an unwarranted invasion of my privacy and would cause me irreparable harm by exposing my personal information. I do not consent to the collection or disclosure of my citizenship status.
11. The Census Bureau is required to produce and publish a comprehensive Privacy Impact Assessment ("PIA") when it begins to develop a new collection of personal data, such as the citizenship status of every person in the United States.
12. I understand that the Census Bureau intends to collect, process, and store personal data concerning citizenship status using five separate Bureau systems: CEN05, CEN08, CEN11, CEN13, and CEN18.

13. On my behalf, EPIC sought the five required Privacy Impact Assessments analyzing the collection, processing, and storage of personal data concerning citizenship status. I also sought the five required Privacy Impact Assessments myself by visiting the webpage where Census Bureau PIAs are published.¹
14. For each of the five CEN systems, the Census Bureau failed to publish a Privacy Impact Assessment that adequately analyzed the collection, processing, and storage of personal data concerning citizenship status. I have therefore been denied information to which I am legally entitled concerning the privacy implications of the Census Bureau's citizenship question.
15. Moreover, I have been irreparably harmed by the Census Bureau's unlawful failure to publish the required Privacy Impact Assessments. I am unable to determine whether the Census Bureau has fully considered or addressed the risks to my privacy, even as the Bureau begins to develop a new collection of personal data that will contain my citizenship status.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed on November 29, 2018



Christopher Wolf

¹ <http://www.osec.doc.gov/opog/privacy/Census-pias.html>.

Exhibit 11

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF COMMERCE,
et al.,

Defendants.

Civ. Action No. 18-2711

DECLARATION OF BRUCE SCHNEIER

I, Bruce Schneier, declare as follows:

1. My name is Bruce Schneier. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I reside in Minneapolis, Minnesota, United States of America.
3. I am a Special Advisor to IBM Security. I am a fellow and lecturer at the Harvard Kennedy School. I am also an author and speaker on security and privacy topics.
4. The Electronic Privacy Information Center (“EPIC”) is a non-profit, public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC’s mission is oversight of government activities that impact individual privacy, free expression, and democratic values. EPIC has a particular interest in preserving legal privacy protections for personal data, including the obligation of federal agencies to conduct privacy impact assessments.
5. I am a member of EPIC. EPIC’s members are distinguished experts in law, technology, and public policy. As a member of EPIC, I serve on the EPIC Advisory Board, participate

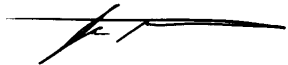
in the activities of EPIC, help finance the activities of EPIC, and provide leadership for EPIC. I also pay annual membership dues, as required by the amended EPIC bylaws.

6. I became an EPIC member because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age. As someone who thinks, works, and writes about digital privacy, EPIC's work on these issues is of special importance to me.
7. EPIC works on my behalf to protect my privacy rights, and I rely on EPIC to obtain and disseminate information about government activities that threaten my privacy.
8. As a resident of the United States, I understand that the Census Bureau intends to ask for my citizenship status on the 2020 Census. By law, I am required to provide a truthful response to such a question.
9. The Census Bureau has indicated that it may disclose my citizenship status to other federal agencies, including for criminal law enforcement purposes.
10. The imminent collection and possible disclosure of my citizenship status by means of the 2020 Census is an unwarranted invasion of my privacy and would cause me irreparable harm by exposing my personal information. I do not consent to the collection or disclosure of my citizenship status.
11. The Census Bureau is required to produce and publish a comprehensive Privacy Impact Assessment ("PIA") when it begins to develop a new collection of personal data, such as the citizenship status of every person in the United States.
12. I understand that the Census Bureau intends to collect, process, and store personal data concerning citizenship status using five separate Bureau systems: CEN05, CEN08, CEN11, CEN13, and CEN18.

13. On my behalf, EPIC sought the five required Privacy Impact Assessments analyzing the collection, processing, and storage of personal data concerning citizenship status. I also sought the five required Privacy Impact Assessments myself by visiting the webpage where Census Bureau PIAs are published.¹
14. For each of the five CEN systems, the Census Bureau failed to publish a Privacy Impact Assessment that adequately analyzed the collection, processing, and storage of personal data concerning citizenship status. I have therefore been denied information to which I am legally entitled concerning the privacy implications of the Census Bureau's citizenship question.
15. Moreover, I have been irreparably harmed by the Census Bureau's unlawful failure to publish the required Privacy Impact Assessments. I am unable to determine whether the Census Bureau has fully considered or addressed the risks to my privacy, even as the Bureau begins to develop a new collection of personal data that will contain my citizenship status.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed on November 30, 2018



Bruce Schneier

¹ <http://www.osec.doc.gov/opog/privacy/Census-pias.html>.

Exhibit 12

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF COMMERCE,
et al.,

Defendants.

Civ. Action No. 18-2711

DECLARATION OF HARRY R. LEWIS

I, Harry R. Lewis, declare as follows:

1. My name is Harry R. Lewis. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I reside in Brookline, Massachusetts United States of America.
3. I am Gordon McKay Professor of Computer Science at Harvard University.
4. The Electronic Privacy Information Center ("EPIC") is a non-profit, public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight of government activities that impact individual privacy, free expression, and democratic values. EPIC has a particular interest in preserving legal privacy protections for personal data, including the obligation of federal agencies to conduct privacy impact assessments.
5. I am a member of EPIC. EPIC's members are distinguished experts in law, technology, and public policy. As a member of EPIC, I serve on the EPIC Advisory Board, participate

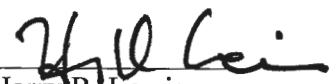
in the activities of EPIC, help finance the activities of EPIC, and provide leadership for EPIC. I also pay annual membership dues, as required by the amended EPIC bylaws.

6. I became an EPIC member because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age. As a professor of computer science, EPIC's work on these issues is of special importance to me.
7. EPIC works on my behalf to protect my privacy rights, and I rely on EPIC to obtain and disseminate information about government activities that threaten my privacy.
8. As a resident of the United States, I understand that the Census Bureau intends to ask for my citizenship status on the 2020 Census. By law, I am required to provide a truthful response to such a question.
9. The Census Bureau has indicated that it may disclose my citizenship status to other federal agencies, including for criminal law enforcement purposes.
10. The imminent collection and possible disclosure of my citizenship status by means of the 2020 Census is an unwarranted invasion of my privacy and would cause me irreparable harm by exposing my personal information. I do not consent to the collection or disclosure of my citizenship status.
11. The Census Bureau is required to produce and publish a comprehensive Privacy Impact Assessment ("PIA") when it begins to develop a new collection of personal data, such as the citizenship status of every person in the United States.
12. I understand that the Census Bureau intends to collect, process, and store personal data concerning citizenship status using five separate Bureau systems: CEN05, CEN08, CEN11, CEN13, and CEN18.

13. On my behalf, EPIC sought the five required Privacy Impact Assessments analyzing the collection, processing, and storage of personal data concerning citizenship status. I also sought the five required Privacy Impact Assessments myself by visiting the webpage where Census Bureau PIAs are published.¹
14. For each of the five CEN systems, the Census Bureau failed to publish a Privacy Impact Assessment that adequately analyzed the collection, processing, and storage of personal data concerning citizenship status. I have therefore been denied information to which I am legally entitled concerning the privacy implications of the Census Bureau's citizenship question.
15. Moreover, I have been irreparably harmed by the Census Bureau's unlawful failure to publish the required Privacy Impact Assessments. I am unable to determine whether the Census Bureau has fully considered or addressed the risks to my privacy, even as the Bureau begins to develop a new collection of personal data that will contain my citizenship status.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed on December 3, 2018


Harry R. Lewis

¹ <http://www.osec.doc.gov/opog/privacy/Census-pias.html>.

Exhibit 13



Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
<https://epic.org>

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to the
U.S. CENSUS BUREAU

2020 Census

83 FR 26643

August 7, 2018

The Electronic Privacy Information Center (“EPIC”) submits these comments in response to the Census Bureau’s notice¹ on the 2020 decennial census.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. The Census implicates numerous privacy issues.² We ask you to consider the risks of personal data being used for purposes that may undermine the integrity, reliability, and purpose of the U.S. census. EPIC specifically asks the Census Bureau to suspend the citizenship question from the 2020 census form until a thorough and updated Privacy Impact Assessment is conducted. So far, the Bureau has failed to demonstrate the data gathered from that particular question will not undermine the privacy rights of those who respond to the census.

EPIC has particular expertise with the misuse of census data after 9-11. And documents EPIC obtained under the Freedom of Information Act led to important reforms at the agency. We urge you not to take our comments lightly.

EPIC supports the work of the Census Bureau and the use of statistical analysis in policymaking and other government initiatives.³ The Census is an essential part of understanding the changing demographics in America. The census helps ensure evidence-based policy decisions and census data is the source of much political and economic planning in the United States. However, it is of the utmost importance the individual privacy is respected. Every effort must be taken to ensure that the personal information of individuals and that census data is not used improperly.

¹ U.S. Census Bureau, *Proposed Information Collection; Comment Request; 2020 Census*, Notice, 83 FR 26643 (June 8, 2018), <https://www.federalregister.gov/documents/2018/06/08/2018-12365/proposed-information-collection-comment-request-2020-census>.

² *The Census and Privacy*, EPIC, <https://epic.org/privacy/census/>.

³ EPIC testified before the Commission on Evidence-Based Policymaking and called for the Commission to adopt innovative privacy safeguards to protect personal data and make informed public policy decisions. Marc Rotenberg, Commission on Evidence-Based Policymaking: Privacy Perspectives, before the National Academies of Science, Sep. 9, 2016, <https://epic.org/privacy/wiretap/RotenbergCEBP-9-16.pdf>.

EPIC knows that the Census Bureau takes its confidentiality requirements seriously⁴ and that some of the strictest privacy laws in the U.S. apply to census data.⁵ But the addition of the citizenship question to the 2020 census raises new privacy issues. The Privacy Impact Assessment for the census indicates that the Bureau has not given proper consideration to these issues.

There has been greater concern about the confidentiality of 2020 census data than in previous decennial censuses. The Census Bureau conducted a study in 2017 that found respondents expressing new concerns including the “Muslim ban,” the dissolution of DACA, and Immigration and Customs Enforcement.⁶ The study found that these concerns were most pronounced among immigrant respondents.⁷

Part I discusses prior abuses of census data, to remind the Bureau that fears of 2020 census data being misused are not abstract. Part II explains why census data should never be used for enforcement purposes. Part III addresses the data integrity issues caused by the addition of the untested question. Part IV describes the Bureau’s Privacy Impact Assessment and why it does not address the privacy risks raised by the addition of the citizenship question.

I. Past Misuses of Census Data

Despite strong census privacy laws, the U.S. has a sordid history of misusing census data to target minority groups. The most egregious misuse of census data was the role it played in the internment of Japanese-Americans during World War II.⁸ In 1943 the Census Bureau complied with a request by the Treasury Secretary for the names and locations of all people of Japanese ancestry in the Washington, D.C., area.⁹ The Bureau should remember this human rights abuse every time another agency requests census data.

After 9-11, EPIC pursued a Freedom of Information Act request about the potential misuse of census data. Documents obtained by EPIC revealed that the Census Bureau had provided the

⁴ Ron Jarmin, *The U.S. Census Bureau’s Commitment to Confidentiality*, Census Blog (May 7, 2018), https://census.gov/newsroom/blogs/director/2018/05/the_u_s_census_bure.html.

⁵ 92 Stat. 915; Public Law 95-416. The Census Bureau cannot disclose “personally identifiable information about an individual to any other individual or agency until 72 years after it was collected for the decennial census.”

⁶ Center for Survey Measurement, MEMORANDUM FOR Associate Directorate for Research and Methodology (ADRM) Respondent Confidentiality Concerns (Sept. 20, 2017), <https://www2.census.gov/cac/nac/meetings/2017-11/Memo-Regarding-Respondent-Confidentiality-Concerns.pdf>.

⁷ *Id.* at 1.

⁸ JR Minkel, *Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II*, Scientific American (March 30, 2007), <https://www.scientificamerican.com/article/confirmed-the-us-census-b/>.

⁹ W. Seltzer and M. Anderson, “Census Confidentiality under the Second War Powers Act (1942-1947).” Paper prepared for presentation at the annual meeting of the Population Association of America, New York, March 29-31, 2007, available at <http://studylib.net/doc/7742798/census-confidentiality-under-the-second-war-powers>.

Department of Homeland Security (“DHS”) with census data on individuals of Arab ancestry.¹⁰ In 2004 EPIC obtained documents revealing that the Census Bureau provided the DHS statistical data on people who identified themselves on the 2000 census as being of Arab ancestry. The special tabulations were prepared specifically for the law enforcement agency. There is no indication that the Department of Homeland Security requested similar information about any other ethnic groups.

One document,¹¹ obtained by EPIC, shows cities with populations of 10,000 or more and with 1,000 or more people who indicated they are of Arab ancestry. For each city, the tabulation provides total population, population of Arab ancestry, and percent of the total population which is of Arab ancestry. The tabulations were produced using data from the 2000 census long-form questionnaire, which goes to only a sample of the population. A second document¹² shows the number of census responses indicating Arab ancestry in certain zip codes throughout the country. The responses indicating Arab ancestry are subdivided into Egyptian, Iraqi, Jordanian, Lebanese, Moroccan, Palestinian, Syrian, Arab/Arabic, and Other Arab. Although this data was not personally identifiable, its disclosure to a law enforcement agency was unethical.

The reason DHS gave for requesting these tabulations was to determine which languages signs should be in at international airports.¹³ Heavily redacted emails¹⁴ between a Census Bureau analyst and a DHS official show that the Bureau gave the documents before the intended purpose for the data was known and that this explanation was given after the tabulations had already been disclosed. The ex-post-facto reason given by DHS seems pretextual.

As a result of these revelations, resulting from EPIC’s FOIA litigation, the Census Bureau revised its policy on sharing statistical information about “sensitive populations” with law enforcement or intelligence agencies. Customs and Border Protection also changed its policy on requesting “information of a sensitive nature from the Census Bureau.”¹⁵

EPIC’s FOIA efforts led the Census Bureau to implement new procedures regarding the release of “potentially sensitive data to requesting law enforcement agencies and organizations or individuals.”¹⁶ EPIC supported those efforts but recognizes also the ongoing concerns about the

¹⁰ *Department of Homeland Security Obtained Data on Arab Americans From Census Bureau*, EPIC, <https://epic.org/privacy/census/foia/>; Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, New York Times, Jul. 30, 2004, <http://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html>.

¹¹ EPIC FOIA, Tabulation 1: “Places with 10,000 or More Population and with 1,000 or More Persons of Arab Ancestry: 2000” https://epic.org/privacy/census/foia/tab_1.pdf.

¹² EPIC FOIA, Tabulation 2: “People of Arab Ancestry by ZIP Code Tabulation Area: 2000” https://epic.org/privacy/census/foia/tab_2.pdf.

¹³ EPIC FOIA, https://epic.org/privacy/census/foia/census_emails.pdf.

¹⁴ *Id.*

¹⁵ U.S. Customs and Border Protection, *Policy for Requesting Information of a Sensitive Nature from the Census Bureau*, Memorandum (Aug. 9, 2004), <https://epic.org/privacy/census/foia/policy.pdf>.

¹⁶ Census Bureau News, “U.S. Census Bureau Announces Policy Regarding Sensitive Data,” press release CB04-145, August 30, 2004; Lynette Clemetson, *Census Policy On Providing Sensitive Data Is Revised*, New York Times, Aug. 31, 2004, <http://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html>.

potential misuse of data collected by government agencies. Amid rising fears that some minority groups may be targeted by law enforcement agencies, your committee should ensure that the data collected by the federal government is not misused.

II. Census Data Should Never Be Used for Enforcement Purposes

Using census data to help enforce laws is a corruption of the decennial census's constitutional purpose. The Department of Justice ("DOJ") requested the citizenship question on the census would allow the agency to better enforce Section 2 of the Voting Rights Act, which bars the dilution of voting power of a minority group through redistricting. DOJ wants census-block-level data for locations where they suspect Section 2 violations have occurred.

The decennial census's statistical purpose is frustrated when other agencies ask it to collect data for other purposes. The DOJ's responsibility to enforce the Voting Rights Act is vital to ensuring fair elections. In its request to the Bureau, the DOJ called the decennial census the "most appropriate vehicle" for collecting data on the citizen voting-age population.¹⁷ EPIC disagrees with this assertion. The decennial census was never intended to be a catch-all data collection to assist other federal agencies. In fact, the statutes concerning the privacy of census data are meant to expressly prohibit this.

If the Census Bureau gets into the business of collecting data because it will assist other federal agencies enforce laws, it will be difficult to stay true to its constitutional purpose of conducting impartial statistical analysis. And it will undermine the integrity, accuracy, and reliability of the census. As a former director of the Bureau succinctly put it thirteen years ago: "The Census Bureau cannot become a quasi-investigatory agency and still perform its basic responsibilities as a statistical agency."¹⁸ The Bureau does not serve an investigatory function and the DOJ (or any other agency) should not expect it to.

III. Data Integrity

When a new question is added this late in preparations for the 2020 census, the burden of proof is on those proposing the new question to establish that it will not impact the integrity of the data collected. The fact that the 2020 census will have an additional question—regardless of what the question asks—is likely to yield lower response rates. As Secretary Ross told Congress: "One of the problems with adding questions is reduced response rates. It may seem counterintuitive, but the

¹⁷ *Re: Request to Reinstate Citizenship Question on 2020 Census Questionnaire* (Dec. 12, 2017), <https://www.documentcloud.org/documents/4340651-Text-of-Dec-2017-DOJ-letter-to-Census.html>.

¹⁸ *Counting the Vote: Should Only U.S. Citizens be Included in Apportioning Our Elected Representatives?*, Hearing Before Subcomm. on Federalism and the Census of the H. Comm. on Gov't Reform, 109th Cong. 77 (2005) (statement of former director of U.S. Census Bureau Kenneth Prewitt).

more things you ask in those forms, the less likely you are to get them in.”¹⁹ And the fact that the new question has not been tested will create further problems with the integrity of the 2020 census data.

Six former directors of the Census Bureau—who served under both Republican and Democrat administrations—wrote to Secretary Ross to warn him that adding a new question to the 2020 census without adequate testing “at this late point in the decennial planning process would put the accuracy of the enumeration and success of the census in all communities at grave risk.”²⁰ The typical process for adding new questions takes multiple years and requires extensive testing. Not only did the citizenship question not go through this process, but it was added after the 2018 End—to—End Census Test was already underway, so it was not even tested in what is meant to be the “dress rehearsal” for the 2020 census.

The former directors said: “even small changes in survey question order, wording, and instructions can have significant, and often unexpected, consequences for the rate, quality, and truthfulness of response.”²¹ But this is a significant change: a new question on a sensitive topic. In addition to a lower response rate, the question would cause an increase in inaccurate responses because “[t]here would be little incentive for non-citizens to offer to the government their actual status.”²²

IV. Insufficiency of Privacy Impact Assessment

The Privacy Impact Assessment (“PIA”) for the 2020 decennial census²³ indicates that the Census Bureau has not undertaken an appropriate analysis of the privacy risks of the citizenship question. “Citizenship” is listed as “other general personal data” that will be collected by the census.²⁴ But, where the Bureau is required to indicate the status of the information system, it selects: “This is an existing information system without changes that create new privacy risks.”²⁵ There is no analysis of the new question.

¹⁹ Rep. Jimmy Gomez Questions Secretary Ross at Oversight Hearing (Oct. 12, 2017), <https://www.c-span.org/video/?c4685802/rep-jimmy-gomez-questions-secretary-ross-oversight-hearing?c4685802/rep-jimmy-gomez-questions-secretary-ross-oversight-hearing/video/>.

²⁰ Letter of Former Directors of U.S. Census Bureau to The Honorable Wilbur L. Ross (Jan. 26, 2018), https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2018/03/27/Editorial-Opinion/Graphics/DOJ_census_ques_request_Former_Directors_ltr_to_Ross.pdf.

²¹ *Id.*

²² Brief of Amici Curiae, *Evenwel v. Abbot*, at 25, <http://www.scotusblog.com/wp-content/uploads/2015/10/Evenwel-FormerCensusBureauDirectorsBrief092515.pdf> (Amici are former directors of the Census Bureau).

²³ U.S. Department of Commerce, U.S. Census Bureau, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division* (July 28, 2018) http://www.osec.doc.gov/opog/privacy/Census%20PIAs/CEN08_PIA_SAOP_Approved.pdf.

²⁴ *Id.* at 3.

²⁵ *Id.* at 2.

The PIA does not satisfy the Department of Commerce's own standards.²⁶ A PIA must be updated "where a system change creates new privacy risks." The Department of Commerce lists nine examples of new privacy risks, and the addition of the citizenship question and the stated purposes for doing so would create at least four of those risks.

The new question would alter the character of the data: "when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)."²⁷ Citizenship data is new information and it is identifiable because it is collected alongside the other information of the person filling out the census form. Immigration status added to the collection of the other demographic data collected by the census undeniably raises the risk to personal privacy. If that privacy were to be violated, that information could be used against the respondent for deportation or other purposes.

The PIA does not acknowledge the privacy risks raised by the new question and the Bureau should conduct a new PIA dealing specifically with the issues raised by the citizenship question.

Conclusion

EPIC recommends that the Census Bureau either remove the citizenship question or conducted a revised Privacy Impact Assessment, taking account of the recently added question, as is required by law. The question raises far-reaching privacy concerns and will also undermine the integrity, reliability and accuracy of the U.S. census.

EPIC has recently pursued related matters concerning the privacy of census data with the Census Bureau that were favorably resolved. We anticipate that will be the outcome here

Sincerely,

/s/ Marc Rotenberg

Marc Rotenberg
EPIC President

/s/ Christine Bannan

Christine Bannan
EPIC Administrative Law and Policy Fellow

²⁶ U.S. Department of Commerce, Office of Privacy and Open Government, *Privacy Compliance* <http://www.osec.doc.gov/opog/privacy/compliance.html>.

²⁷ *Id.* "Alteration in Character of Data" is the ninth example in the list of privacy risks.

Exhibit 14



Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
<https://epic.org>

October 2, 2018

The Honorable Ron Johnson, Chairman
The Honorable Claire McCaskill, Ranking Member
U.S. Senate Committee on Homeland Security & Government Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill:

We write to you regarding the nomination hearing of Steven D. Dillingham to be Director of the Census¹ EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC takes no position for or against the nominee. However, the Census implicates numerous privacy issues.² EPIC specifically asks the Census Bureau to suspend the citizenship question from the 2020 census form until a thorough and updated Privacy Impact Assessment is conducted. The Bureau has failed to demonstrate the data gathered from that particular question will not undermine the privacy rights of those who respond to the census.

EPIC supports the work of the Census Bureau and the use of statistical analysis in policymaking and other government initiatives.³ The Census is an essential part of understanding the changing demographics in America. The census helps ensure evidence-based policy decisions and census data is the source of much political and economic planning in the United States. However, it is of the utmost importance the individual privacy is respected. Every effort must be taken to ensure that the personal information of individuals and that census data is not used improperly.

Through a Freedom of Information Act request EPIC has obtained documents regarding Secretary Ross's decision to add the citizenship question to the 2020 Census.⁴ The documents obtained by EPIC reflect the varying opinions from lawmakers, scientists, and immigration groups

¹ *Nomination of Steven D. Dillingham to be Director of the Census*, 115th Cong. (2018), S. Comm. on Homeland Security & Governmental Affairs, <https://www.hsgac.senate.gov/hearings/09/25/2018/nominations> (October 3, 2018).

² *The Census and Privacy*, EPIC, <https://epic.org/privacy/census/>.

³ EPIC testified before the Commission on Evidence-Based Policymaking and called for the Commission to adopt innovative privacy safeguards to protect personal data and make informed public policy decisions. Marc Rotenberg, Commission on Evidence-Based Policymaking: Privacy Perspectives, before the National Academies of Science, Sep. 9, 2016, <https://epic.org/privacy/wiretap/RotenbergCEBP-9-16.pdf>.

⁴ FOIA Production 1, <https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-1.pdf>; FOIA Production 2, <https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-2.pdf>; FOIA Production 3, <https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-3.pdf>; FOIA Production 4, <https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-4.pdf>.

about the proposal. The documents also reveal that Kris Kobach, former Vice Chair of the now-defunct Presidential Advisory Commission on Election Integrity, urged Secretary Ross "on the direction of Steve Bannon" to add the citizenship question. According to an analysis conducted by the Census Bureau, the impact of asking about citizenship would be "very costly, harms the quality of the census count, and would use substantially less accurate citizenship data than are available" from other government resources.

I. Past Misuses of Census Data

There is substantial concern about the confidentiality of census data as a result of Secretary Ross's decision to add a citizenship question to the 2020 census. Despite strong census privacy laws, the U.S. has a sordid history of misusing census data to target minority groups. The most egregious misuse of census data was the role it played in the internment of Japanese-Americans during World War II.⁵ In 1943 the Census Bureau complied with a request by the Treasury Secretary for the names and locations of all people of Japanese ancestry in the Washington, D.C., area.⁶ The Bureau should remember this human rights abuse every time another agency requests census data.

EPIC has a strong interest in the government's use of Census data. After 9-11, EPIC pursued a Freedom of Information Act request about the transfer of Census data to the Department of Homeland Security. Documents obtained by EPIC revealed that the Census Bureau had provided the Department of Homeland Security ("DHS") with census data on individuals of Arab ancestry.⁷ In 2004 EPIC obtained documents revealing that the Census Bureau provided the DHS statistical data on people who identified themselves on the 2000 census as being of Arab ancestry. The special tabulations were prepared specifically for the law enforcement agency. There is no indication that the Department of Homeland Security requested similar information about any other ethnic groups.

One document,⁸ obtained by EPIC, shows cities with populations of 10,000 or more and with 1,000 or more people who indicated they are of Arab ancestry. For each city, the tabulation provides total population, population of Arab ancestry, and percent of the total population which is of Arab ancestry. The tabulations were produced using data from the 2000 census long-form questionnaire, which goes to only a sample of the population. A second document⁹ shows the number of census responses indicating Arab ancestry in certain zip codes throughout the country. The responses

⁵ JR Minkel, *Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II*, Scientific American (March 30, 2007), <https://www.scientificamerican.com/article/confirmed-the-us-census-b/>.

⁶ W. Seltzer and M. Anderson, "Census Confidentiality under the Second War Powers Act (1942-1947)." Paper prepared for presentation at the annual meeting of the Population Association of America, New York, March 29-31, 2007, available at <http://studylib.net/doc/7742798/census-confidentiality-under-the-second-war-powers>.

⁷ *Department of Homeland Security Obtained Data on Arab Americans From Census Bureau*, EPIC, <https://epic.org/privacy/census/foia/>; Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, New York Times, Jul. 30, 2004, <http://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html>.

⁸ EPIC FOIA, Tabulation 1: "Places with 10,000 or More Population and with 1,000 or More Persons of Arab Ancestry: 2000" https://epic.org/privacy/census/foia/tab_1.pdf.

⁹ EPIC FOIA, Tabulation 2: "People of Arab Ancestry by ZIP Code Tabulation Area: 2000" https://epic.org/privacy/census/foia/tab_2.pdf.

indicating Arab ancestry are subdivided into Egyptian, Iraqi, Jordanian, Lebanese, Moroccan, Palestinian, Syrian, Arab/Arabic, and Other Arab. Although this data was not personally identifiable, its disclosure to a law enforcement agency was unethical.

The reason DHS gave for requesting these tabulations was to determine which languages signs should be in at international airports.¹⁰ Heavily redacted emails¹¹ between a Census Bureau analyst and a DHS official show that the Bureau gave the documents before the intended purpose for the data was known and that this explanation was given after the tabulations had already been disclosed. The ex-post-facto reason given by DHS seems pretextual.

As a result of these revelations, resulting from EPIC's FOIA litigation, the Census Bureau revised its policy on sharing statistical information about "sensitive populations" with law enforcement or intelligence agencies. Customs and Border Protection also changed its policy on requesting "information of a sensitive nature from the Census Bureau."¹²

II. Census Data Should Never Be Used for Enforcement Purposes

Using census data to help enforce laws is a corruption of the decennial census's constitutional purpose. The Department of Justice ("DOJ") requested the citizenship question on the census would allow the agency to better enforce Section 2 of the Voting Rights Act, which bars the dilution of voting power of a minority group through redistricting. DOJ wants census-block-level data for locations where they suspect Section 2 violations have occurred.

The decennial census's statistical purpose is frustrated when other agencies ask it to collect data for other purposes. The DOJ's responsibility to enforce the Voting Rights Act is vital to ensuring fair elections. In its request to the Bureau, the DOJ called the decennial census the "most appropriate vehicle" for collecting data on the citizen voting-age population.¹³ EPIC disagrees with this assertion. The decennial census was never intended to be a catch-all data collection to assist other federal agencies. In fact, the statutes concerning the privacy of census data are meant to expressly prohibit this.

If the Census Bureau gets into the business of collecting data because it will assist other federal agencies enforce laws, it will be difficult to stay true to its constitutional purpose of conducting impartial statistical analysis. And it will undermine the integrity, accuracy, and reliability of the census. As a former director of the Bureau succinctly put it thirteen years ago: "The Census Bureau cannot become a quasi-investigatory agency and still perform its basic responsibilities as a statistical agency."¹⁴ The Bureau does not serve an investigatory function and the DOJ (or any other agency) should not expect it to.

¹⁰ EPIC FOIA, https://epic.org/privacy/census/foia/census_emails.pdf.

¹¹ *Id.*

¹² U.S. Customs and Border Protection, *Policy for Requesting Information of a Sensitive Nature from the Census Bureau*, Memorandum (Aug. 9, 2004), <https://epic.org/privacy/census/foia/policy.pdf>.

¹³ *Re: Request to Reinstate Citizenship Question on 2020 Census Questionnaire* (Dec. 12, 2017), <https://www.documentcloud.org/documents/4340651-Text-of-Dec-2017-DOJ-letter-to-Census.html>.

¹⁴ *Counting the Vote: Should Only U.S. Citizens be Included in Apportioning Our Elected Representatives?*, Hearing Before Subcomm. on Federalism and the Census of the H. Comm. on Gov't Reform, 109th Cong. 77 (2005) (statement of former director of U.S. Census Bureau Kenneth Prewitt).

IV. Insufficiency of Privacy Impact Assessment

The Privacy Impact Assessment (“PIA”) for the 2020 decennial census¹⁵ indicates that the Census Bureau has not undertaken an appropriate analysis of the privacy risks of the citizenship question. “Citizenship” is listed as “other general personal data” that will be collected by the census.¹⁶ But, where the Bureau is required to indicate the status of the information system, it selects: “This is an existing information system without changes that create new privacy risks.”¹⁷ There is no analysis of the new question.

The PIA does not satisfy the Department of Commerce’s own standards.¹⁸ A PIA must be updated “where a system change creates new privacy risks.” The Department of Commerce lists nine examples of new privacy risks, and the addition of the citizenship question and the stated purposes for doing so would create at least four of those risks.

The new question would alter the character of the data: “when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).”¹⁹ Citizenship data is new information and it is identifiable because it is collected alongside the other information of the person filling out the census form. Immigration status added to the collection of the other demographic data collected by the census undeniably raises the risk to personal privacy. If that privacy were to be violated, that information could be used against the respondent for deportation or other purposes. The PIA does not acknowledge the privacy risks raised by the new question and the Bureau should conduct a new PIA dealing specifically with the issues raised by the citizenship question.

EPIC looks forward to working with the Committee to ensure that the census data provides the maximum benefit to the American public while minimizing the privacy risks. We ask that this letter from EPIC be entered in the hearing record.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Christine Bannan
Christine Bannan
EPIC Consumer Protection Counsel

¹⁵ U.S. Department of Commerce, U.S. Census Bureau, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division* (July 28, 2018)

http://www.osec.doc.gov/opog/privacy/Census%20PIAs/CEN08_PIA_SAOP_Approved.pdf.

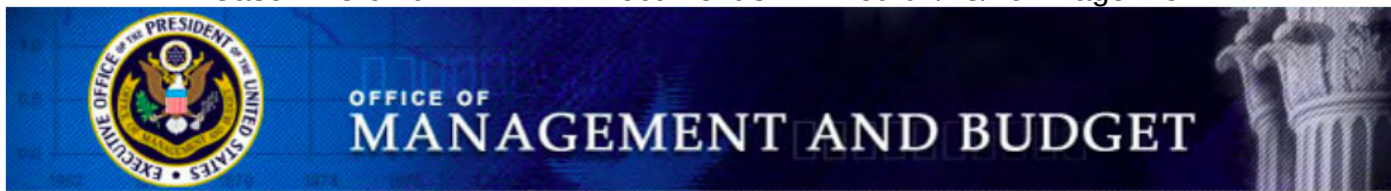
¹⁶ *Id.* at 3.

¹⁷ *Id.* at 2.

¹⁸ U.S. Department of Commerce, Office of Privacy and Open Government, *Privacy Compliance* <http://www.osec.doc.gov/opog/privacy/compliance.html>.

¹⁹ *Id.* “Alteration in Character of Data” is the ninth example in the list of privacy risks.

Exhibit 15



September 26, 2003

M-03-22

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director



SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

Background

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail Eva_Kleederman@omb.eop.gov.

Attachments

[Attachment A](#)
[Attachment B](#)
[Attachment C](#)
[Attachment D](#)

Attachment A

E-Government Act Section 208 Implementation Guidance

I. General

A. Requirements. Agencies are required to:

1. conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),
2. post privacy policies on agency websites used by the public (see Section III),

3. translate privacy policies into a standardized machine-readable format (see Section IV), and
4. report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).

B. Application. This guidance applies to:

1. all executive branch departments and agencies (“agencies”) and their contractors that use information technology or that operate websites for purposes of interacting with the public;
2. relevant cross-agency initiatives, including those that further electronic government.

C.

Modifications to Current Guidance. Where indicated, this Memorandum modifies the following three memoranda, which are replaced by this guidance (see summary of modifications at Attachment D):

1. [Memorandum 99-05](#) (January 7, 1999), directing agencies to examine their procedures for ensuring the privacy of personal information in federal records and to designate a senior official to assume primary responsibility for privacy policy;
2. [Memorandum 99-18](#) (June 2, 1999), concerning posting privacy policies on major entry points to government web sites as well as on any web page collecting substantial personal information from the public; and
3. [Memorandum 00-13](#) (June 22, 2000), concerning (i) the use of tracking technologies such as persistent cookies and (ii) parental consent consistent with the Children’s Online Privacy Protection Act (“COPPA”).

II. Privacy Impact Assessment

A. Definitions.

1. Individual - means a citizen of the United States or an alien lawfully admitted for permanent residence.¹
2. Information in identifiable form- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).²
3. Information technology (IT) - means, as defined in the Clinger-Cohen Act³, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. Major information system - embraces “large” and “sensitive” information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency’s programs, finances, property or other resources.
5. National Security Systems - means, as defined in the Clinger-Cohen Act⁴, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.
6. Privacy Impact Assessment (PIA)- is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
7. Privacy policy in standardized machine-readable format- means a statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.

B. When to conduct a PIA:⁵

1. The E-Government Act requires agencies to conduct a PIA before:
 - a. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
 - b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).
2. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

- a. Conversions - when converting paper-based records to electronic systems;
 - b. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
 - c. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
 - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
 - d. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
 - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
 - e. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
 - f. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
 - g. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA:
 - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
 - h. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
 - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
 - i. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)
3. No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged, as in the following circumstances:
- a. for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants);⁶
 - b. for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or obtaining additional information;
 - c. for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);
 - d. when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;
 - e. when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;
 - f. if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form;
 - g. for minor changes to a system or collection that do not create new privacy risks.
4. Update of PIAs: Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

C. Conducting a PIA.

1. Content.

a. PIAs must analyze and describe:

- i. what information is to be collected (e.g., nature and source);
- ii. why the information is being collected (e.g., to determine eligibility);
- iii. intended use of the information (e.g., to verify existing data);
- iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
- v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
- vi. how the information will be secured (e.g., administrative and technological controls⁷); and
- vii. whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

b. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

2. Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:

a. Specificity. The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.

i. IT development stage. PIAs conducted at this stage:

- 1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
- 2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
- 3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.

ii. Major information systems. PIAs conducted for these systems should reflect more extensive analyses of:

- 1. the consequences of collection and flow of information,
- 2. the alternatives to collection and handling as designed,
- 3. the appropriate measures to mitigate risks identified for each alternative and,
- 4. the rationale for the final design choice or business process.

iii. Routine database systems. Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.

b. Information life cycle analysis/collaboration. Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.

3. Review and publication.

a. Agencies must ensure that:

- i. the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);
- ii. for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300⁸); and
- iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).
 - 1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment⁹. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).
 - 2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such

information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

D. Relationship to requirements under the Paperwork Reduction Act (PRA)¹⁰.

1. Joint Information Collection Request (ICR) and PIA. Agencies undertaking new electronic information collections may conduct and submit the PIA to OMB, and make it publicly available, as part of the SF83 Supporting Statement (the request to OMB to approve a new agency information collection).
2. If Agencies submit a Joint ICR and PIA:
 - a. All elements of the PIA must be addressed and identifiable within the structure of the Supporting Statement to the ICR, including:
 - i. a description of the information to be collected in the response to Item 1 of the Supporting Statement¹¹;
 - ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement¹²;
 - iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement¹³;
 - iv. a discussion in item 10 of the Supporting Statement of:
 1. whether individuals are informed that providing the information is mandatory or voluntary
 2. opportunities to consent, if any, to sharing and submission of information;
 3. how the information will be secured; and
 4. whether a system of records is being created under the Privacy Act¹⁴.
 - b. For additional information on the requirements of an ICR, please consult your agency's organization responsible for PRA compliance.
3. Agencies need not conduct a new PIA for simple renewal requests for information collections under the PRA. As determined by reference to section II.B.2. above, agencies must separately consider the need for a PIA when amending an ICR to collect information that is significantly different in character from the original collection.

E. Relationship to requirements under the Privacy Act of 1974, 5 U.S. C. 552a.

1. Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by subsection (e)(4) of the Privacy Act, in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).
2. Agencies, in addition, may make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.
3. Agencies must separately consider the need for a PIA when issuing a change to a SOR notice (e.g., a change in the type or category of record added to the system may warrant a PIA).

III. Privacy Policies on Agency Websites

- A. Privacy Policy Clarification. To promote clarity to the public, agencies are required to refer to their general web site notices explaining agency information handling practices as the "Privacy Policy."
- B. Effective Date. Agencies are expected to implement the following changes to their websites by December 15, 2003.
- C. Exclusions: For purposes of web privacy policies, this guidance does not apply to:
 1. information other than "government information" as defined in [OMB Circular A-130](#);
 2. agency intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);
 3. national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-government Act).
- D. Content of Privacy Policies.
 1. Agency Privacy Policies must comply with guidance issued in OMB [Memorandum 99-18](#) and must now also include the following two new content areas:
 - a. Consent to collection and sharing¹⁵. Agencies must now ensure that privacy policies:
 - i. inform visitors whenever providing requested information is voluntary;
 - ii. inform visitors how to grant consent for use of voluntarily-provided information; and
 - iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
 - b. Rights under the Privacy Act or other privacy laws¹⁶. Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
 - i. in the body of the web privacy policy;

- ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
 - iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
- 2. Agency Privacy Policies must continue to address the following, modified, requirements:
 - a. Nature, purpose, use and sharing of information collected . Agencies should follow existing policies (issued in [OMB Memorandum 99-18](#)) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
 - i. Privacy Act information. When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
 - 1. at the point of collection, or
 - 2. via link to the agency's general Privacy Policy¹⁸.
 - ii. "Privacy Act Statements." Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
 - iii. Automatically Collected Information (site management data). Agency Privacy Policies must specify what information the agency collects automatically (i.e., user's IP address, location, and time of visit) and identify the use for which it is collected (i.e., site management or security purposes).
 - iv. Interaction with children: Agencies that provide content to children under 13 and that collect personally identifiable information from these visitors should incorporate the requirements of the Children's Online Privacy Protection Act ("COPPA") into their Privacy Policies (see Attachment C)¹⁹.
 - v. Tracking and customization activities. Agencies are directed to adhere to the following modifications to [OMB Memorandum 00-13](#) and the OMB follow-up guidance letter dated [September 5, 2000](#):
 - 1. Tracking technology prohibitions:
 - a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
 - b. agency heads may approve, or may authorize the heads of sub-agencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:
 - the nature of the information collected;
 - the purpose and use for the information;
 - whether and to whom the information will be disclosed; and
 - the privacy safeguards applied to the information collected.
 - c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII)²⁰.
 - 2. The following technologies are not prohibited:
 - a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
 - b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
 - the purpose of the tracking (i.e., customization of the site);
 - that accepting the customizing feature is voluntary;
 - that declining the feature still permits the individual to use the site; and
 - the privacy safeguards in place for handling the information collected.
 - c. Agency use of password access to information that does not involve "persistent cookies" or similar technology.
 - vi. Law enforcement and homeland security sharing: Consistent with current practice, Internet privacy policies may reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security and national security activities.
 - b. Security of the information²¹. Agencies should continue to comply with existing requirements for computer security in administering their websites²² and post the following information in their Privacy Policy:

- i. in clear language, information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and
- ii. in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)

E. Placement of notices. Agencies should continue to follow the policy identified in [OMB Memorandum 99-18](#) regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:

1. their principal web site;
2. any known, major entry points to their sites;
3. any web page that collects substantial information in identifiable form.

F. Clarity of notices. Consistent with [OMB Memorandum 99-18](#), privacy policies must be:

1. clearly labeled and easily accessed;
2. written in plain language; and
3. made clear and easy to understand, whether by integrating all information and statements into a single posting, by layering a short “highlights” notice linked to full explanation, or by other means the agency determines is effective.

IV. Privacy Policies in Machine-Readable Formats

A. Actions.

1. Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make an informed choice about whether to conduct business with that site.
2. OMB encourages agencies to adopt other privacy protective tools that become available as the technology advances.

B. Reporting Requirement. Agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format. The timetable must include achievable milestones that show the agency's progress toward implementation over the next year. Agencies must include this timetable in their reports to OMB (see Section VII).

V. Privacy Policies Incorporated by this Guidance

In addition to the particular actions discussed above, this guidance reiterates general directives from previous OMB Memoranda regarding the privacy of personal information in federal records and collected on federal web sites. Specifically, existing policies continue to require that agencies:

- A. assure that their uses of new information technologies sustain, and do not erode, the protections provided in all statutes relating to agency use, collection, and disclosure of personal information;
- B. assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- C. evaluate legislative proposals involving collection, use and disclosure of personal information by the federal government for consistency with the Privacy Act of 1974;
- D. evaluate legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles;
- E. ensure full adherence with stated privacy policies.

VI. Agency Privacy Activities/Designation of Responsible Official

Because of the capability of information technology to capture and disseminate information in an instant, all federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form. In addition, implementing the privacy provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act and project officers located in disparate organizations within agencies. Clear leadership and authority are essential.

Accordingly, this guidance builds on policy introduced in Memorandum 99-05 in the following ways:

A. Agencies must:

1. inform and educate employees and contractors of their responsibility for protecting information in identifiable form;
2. identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.
3. designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance.
4. designate an appropriate official (or officials, as appropriate) to serve as the “reviewing official(s)” for agency PIAs.

- B. OMB leads a committee of key officials involved in privacy that reviewed and helped shape this guidance and that will review and help shape any follow-on privacy and web-privacy-related guidance. In addition, as part of overseeing agencies' implementation of section 208, OMB will rely on the CIO Council to collect information on agencies' initial experience in preparing PIAs, to share experiences, ideas, and promising practices as well as identify any needed revisions to OMB's guidance on PIAs.

VII. Reporting Requirements

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. The first reports are due to OMB by December 15, 2003. All agencies that use information technology systems and conduct electronic information collection activities must complete a report on compliance with this guidance, whether or not they submit budgets to OMB.

Reports must address the following four elements:

- A. Information technology systems or information collections for which PIAs were conducted. Include the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all (if in summary form or not at all, explain), and, if made available in conjunction with an ICR or SOR, the publication date.
- B. Persistent tracking technology uses. If persistent tracking technology is authorized, include the need that compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the actual privacy policy notification of such use.
- C. Agency achievement of goals for machine readability: Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.
- D. Contact information. Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for information technology/web matters and the individual (name and title) primarily responsible for privacy policies.

Attachment B
E-Government Act of 2002
Pub. L. No. 107-347, Dec. 17, 2002

SEC. 208. PRIVACY PROVISIONS.

A. PURPOSE. — The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

B. PRIVACY IMPACT ASSESSMENTS.—

1. RESPONSIBILITIES OF AGENCIES.—

- a. IN GENERAL.—An agency shall take actions described under subparagraph (b) before—
 - i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
 - ii. initiating a new collection of information that—
 1. will be collected, maintained, or disseminated using information technology; and
 2. includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.
- b. AGENCY ACTIVITIES. —To the extent required under subparagraph (a), each agency shall—
 - i. conduct a privacy impact assessment;
 - ii. ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
 - iii. if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.
- c. SENSITIVE INFORMATION. —Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.
- d. COPY TO DIRECTOR. —Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

2. CONTENTS OF A PRIVACY IMPACT ASSESSMENT. —

- a. IN GENERAL. —The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.
- b. GUIDANCE. — The guidance shall—
 - i. ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
 - ii. require that a privacy impact assessment address—
 1. what information is to be collected;
 2. why the information is being collected;
 3. the intended use of the agency of the information;
 4. with whom the information will be shared;

5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
6. how the information will be secured; and
7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the 'Privacy Act').

3. RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

- a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
- b. oversee the implementation of the privacy impact assessment process throughout the Government; and
- c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

C. PRIVACY PROTECTIONS ON AGENCY WEBSITES. —

1. PRIVACY POLICIES ON WEBSITES. —

- a. GUIDELINES FOR NOTICES. —The Director shall develop guidance for privacy notices on agency websites used by the public.
- b. CONTENTS. —The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
 - i. what information is to be collected;
 - ii. why the information is being collected;
 - iii. the intended use of the agency of the information;
 - iv. with whom the information will be shared;
 - v. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
 - vi. how the information will be secured; and
 - vii. the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act'), and other laws relevant to the protection of the privacy of an individual.

2. PRIVACY POLICIES IN MACHINE-READABLE FORMATS. — The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

D. DEFINITION. —In this section, the term 'identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Attachment C

This attachment is a summary by the Federal Trade Commission of its guidance regarding federal agency compliance with the Children's Online Privacy Protection Act (COPPA).

The hallmarks of COPPA for purposes of federal online activity are (i) notice of information collection practices (ii) verifiable parental consent and (iii) access, as generally outlined below:

- Notice of Information Collection Practices

Agencies whose Internet sites offer a separate children's area and collect personal information from them must post a clear and prominent link to its Internet privacy policy on the home page of the children's area and at each area where it collects personal information from children. The privacy policy should provide the name and contact information of the agency representative required to respond to parental inquiries about the site. Importantly, the privacy policy should inform parents about the kinds of information collected from children, how the information is collected (directly, or through cookies), how the information is used, and procedures for reviewing/deleting the information obtained from children.

In addition, the privacy policy should inform parents that only the minimum information necessary for participation in the activity is collected from the child. In addition to providing notice by posting a privacy policy, notice of an Internet site's information collection practices must be sent directly to a parent when a site is requesting parental consent to collection personal information from a child. This direct notice should tell parents that the site would like to collect personal information from their child, that their consent is required for this collection, and how consent can be provided. The notice should also contain the information set forth in the site's privacy policy, or provide an explanatory link to the privacy policy.

- Verifiable Parental Consent

With limited exceptions, agencies must obtain parental consent before collecting any personal information from children under the age of 13. If agencies are using the personal information for their internal use only, they may obtain parental consent through an e-mail message from the parent, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, agencies might seek confirmation from a parent in a delayed confirmatory e-mail, or confirm the parent's consent by letter or phone call²³.

However, if agencies disclose the personal information to third parties or the public (through chat rooms or message boards), only the most reliable methods of obtaining consent must be used. These methods include: (i) obtaining a signed form from the parent via postal mail or facsimile, (ii) accepting and verifying a credit card number in connection with a transaction, (iii) taking calls from parents through a toll-free telephone number staffed by trained personnel, or (iv) email accompanied by digital signature.

Although COPPA anticipates that private sector Internet operators may share collected information with third parties (for marketing or other commercial purposes) and with the public (through chat rooms or message boards), as a general principle, federal agencies collect information from children only for purposes of the immediate online activity or other, disclosed, internal agency use. (Internal agency use of collected information would include release to others who use it solely to provide support for the internal operations of the site or service, including technical support and order fulfillment.) By analogy to COPPA and consistent with the Privacy Act, agencies may not use information collected from children in any manner not initially disclosed and for which explicit parental consent has not been obtained. Agencies' Internet privacy policies should reflect these disclosure and consent principles.

COPPA's implementing regulations include several exceptions to the requirement to obtain advance parental consent where the Internet operator (here, the agency) collects a child's email address for the following purposes: (i) to provide notice and seek consent, (ii) to respond to a one-time request from a child before deleting it, (iii) to respond more than once to a specific request, e.g., for a subscription to a newsletter, as long as the parent is notified of, and has the opportunity to terminate a continuing series of communications, (iv) to protect the safety of a child, so long as the parent is notified and given the opportunity to prevent further use of the information, and (v) to protect the security or liability of the site or to respond to law enforcement if necessary.

Agencies should send a new notice and request for consent to parents any time the agency makes material changes in the collection or use of information to which the parent had previously agreed. Agencies should also make clear to parents that they may revoke their consent, refuse to allow further use or collection of the child's personal information and direct the agency to delete the information at any time.

- Access

At a parent's request, agencies must disclose the general kinds of personal information they collect online from children as well as the specific information collected from a child. Agencies must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information, e.g., obtaining signed hard copy of identification, accepting and verifying a credit card number, taking calls from parents on a toll-free line staffed by trained personnel, email accompanied by digital signature, or email accompanied by a PIN or password obtained through one of the verification methods above.

In adapting the provisions of COPPA to their Internet operations, agencies should consult the FTC's web site at <http://www.ftc.gov/privacy/privacyinitiatives/childrens.html> or call the COPPA compliance telephone line at (202) 326-3140.

Attachment D

Summary of Modifications to Prior Guidance

This Memorandum modifies prior guidance in the following ways:

* Internet Privacy Policies ([Memorandum 99-18](#)):

- must identify when tracking technology is used to personalize the interaction, and explain the purpose of the feature and the visitor's option to decline it.
- must clearly explain when information is maintained and retrieved by personal identifier in a Privacy Act system of records; must provide (or link to) a Privacy Act statement (which may be subsumed within agency's Internet privacy policy) where Privacy Act information is solicited.
- should clearly explain an individual's rights under the Privacy Act if solicited information is to be maintained in a Privacy Act system of records; information about rights under the Privacy Act may be provided in the body of the web privacy policy or via link to the agency's published systems notice and Privacy Act regulation or other summary of rights under the Privacy Act (notice and explanation of rights under other privacy laws should be handled in the same manner).
- when a Privacy Act Statement is not required, must link to the agency's Internet privacy policy explaining the purpose of the collection and use of the information (point-of-collection notice at agency option).

- must clearly explain where the user may consent to the collection or sharing of information and must notify users of any available mechanism to grant consent.
- agencies must undertake to make their Internet privacy policies “readable” by privacy protection technology and report to OMB their progress in that effort.
- must adhere to the regulatory requirements of the Children’s Online Privacy Protection Act (COPPA) when collecting information electronically from children under age 13.

*Tracking Technology ([Memorandum 00-13](#)):

- prohibition against tracking visitors’ Internet use extended to include tracking by any means (previous guidance addressed only “persistent cookies”).? authority to waive the prohibition on tracking in appropriate circumstances may be retained by the head of an agency, or may be delegated to (i) senior official(s) reporting directly to the agency head, or to (ii) the heads of sub-agencies.? agencies must report the use of tracking technology to OMB, identifying the circumstances, safeguards and approving official.
- agencies using customizing technology must explain the use, voluntary nature of and the safeguards applicable to the customizing device in the Internet privacy policy.
- agency heads or their designees may approve the use of persistent tracking technology to customize Internet interactions with the government.

* Privacy responsibilities ([Memorandum 99-05](#))

- agencies to identify individuals with day-to-day responsibility for implementing the privacy provisions of the E-Government Act, the Privacy Act and any other applicable statutory privacy regime.
- agencies to report to OMB the identities of senior official(s) primarily responsible for implementing and coordinating information technology/web policies and privacy policies.

-
1. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.
 2. Information in identifiable form is defined in section 208(d) of the Act as “any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.” Information “permitting the physical or online contacting of a specific individual” (see section 208(b)(1)(A)(ii)(II)) is the same as “information in identifiable form.”
 3. Clinger-Cohen Act of 1996, 40 U.S.C. 11101(6).
 4. Clinger-Cohen Act of 1996, 40 U.S.C. 11103.
 5. In addition to these statutorily prescribed activities, the E-Government Act authorizes the Director of OMB to require agencies to conduct PIAs of existing electronic information systems or ongoing collections of information in identifiable form as the Director determines appropriate. (see section 208(b)(3)(C)).
 6. Information in identifiable form about government personnel generally is protected by the Privacy Act of 1974. Nevertheless, OMB encourages agencies to conduct PIAs for these systems as appropriate.
 7. Consistent with agency requirements under the Federal Information Security Management Act, agencies should: (i) affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured, (ii) acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls, (iii) describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information, and (iv) provide a point of contact for any additional questions from users. Given the potential sensitivity of security-related information, agencies should ensure that the IT security official responsible for the security of the system and its information reviews the language before it is posted.
 8. PIAs that comply with the statutory requirements and previous versions of this Memorandum are acceptable for agencies’ FY 2005 budget submissions.
 9. Section 208(b)(1)(C).
 10. See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.
 11. Item 1 of the Supporting Statement reads: “Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.”
 12. Item 2 of the Supporting Statement reads: “Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.”
 13. Item 2 of the Supporting Statement reads: “Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.”
 14. Item 10 of the Supporting Statement reads: “Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.”
 15. Section 208(c)(1)(B)(v).
 16. Section 208(c)(1)(B)(vii).

17. Section 208(c)(1)(B)(i-iv).
18. When multiple Privacy Act Statements are incorporated in a web privacy policy, a point-of-collection link must connect to the Privacy Act Statement pertinent to the particular collection.
19. Attachment C contains a general outline of COPPA's regulatory requirements. Agencies should consult the Federal Trade Commission's COPPA compliance telephone line at (202)-326-3140 or website for additional information at: <http://www.ftc.gov/privacy/privacyinitiatives/childrens.html>.
20. Consistent with current practice, the agency head or designee may limit, as appropriate, notice and reporting of tracking activities that the agency has properly approved and which are used for authorized law enforcement, national security and/or homeland security purposes.
21. Section 208(c)(1)(B)(vi).
22. Federal Information Security Management Act of 2002 (Title III of P.L. 107-347), OMB's related security guidance and policies (Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources") and standards and guidelines development by the National Institute of Standards and Technologies.
23. This standard was set to expire in April 2002, at which time the most verifiable methods of obtaining consent would have been required; however, in a Notice of Proposed Rulemaking, published in the Federal Register on October 31, 2001, the FTC has proposed that this standard be extended until April 2004. 66 Fed. Reg. 54963.

Exhibit 16

This is the official form for all the people at this address.
It is quick and easy, and your answers are protected by law.

Use a blue or black pen.

Start here

The Census must count every person living in the United States on April 1, 2010.

Before you answer Question 1, count the people living in this house, apartment, or mobile home using our guidelines.

- Count all people, including babies, who live and sleep here most of the time.

The Census Bureau also conducts counts in institutions and other places, so:

- Do not count anyone living away either at college or in the Armed Forces.
- Do not count anyone in a nursing home, jail, prison, detention facility, etc., on April 1, 2010.
- Leave these people off your form, even if they will return to live here after they leave college, the nursing home, the military, jail, etc. Otherwise, they may be counted twice.

The Census must also include people without a permanent place to stay, so:

- If someone who has no permanent place to stay is staying here on April 1, 2010, count that person. Otherwise, he or she may be missed in the census.

1. How many people were living or staying in this house, apartment, or mobile home on April 1, 2010?

Number of people =

2. Were there any additional people staying here April 1, 2010 that you did not include in Question 1?

Mark ☒ all that apply.

- ☐ Children, such as newborn babies or foster children
- ☐ Relatives, such as adult children, cousins, or in-laws
- ☐ Nonrelatives, such as roommates or live-in baby sitters
- ☐ People staying here temporarily
- ☐ No additional people

3. Is this house, apartment, or mobile home —

Mark ☒ ONE box.

- ☐ Owned by you or someone in this household with a mortgage or loan? *Include home equity loans.*
- ☐ Owned by you or someone in this household free and clear (without a mortgage or loan)?
- ☐ Rented?
- ☐ Occupied without payment of rent?

4. What is your telephone number? We may call if we don't understand an answer.

Area Code + Number

- -

OMB No. 0607-0919-C: Approval Expires 12/31/2011.

Form **D-61** (1-15-2009)

5. Please provide information for each person living here. Start with a person living here who owns or rents this house, apartment, or mobile home. If the owner or renter lives somewhere else, start with any adult living here. This will be Person 1.

What is Person 1's name? *Print name below.*

Last Name

First Name

MI

6. What is Person 1's sex? Mark ☒ ONE box.

- ☐ Male ☐ Female

7. What is Person 1's age and what is Person 1's date of birth?

Please report babies as age 0 when the child is less than 1 year old.

Print numbers in boxes.

Age on April 1, 2010

Month

Day

Year of birth

→ **NOTE: Please answer BOTH Question 8 about Hispanic origin and Question 9 about race. For this census, Hispanic origins are not races.**

8. Is Person 1 of Hispanic, Latino, or Spanish origin?

- ☐ No, not of Hispanic, Latino, or Spanish origin
- ☐ Yes, Mexican, Mexican Am., Chicano
- ☐ Yes, Puerto Rican
- ☒ Yes, Cuban
- ☐ Yes, another Hispanic, Latino, or Spanish origin — *Print origin, for example, Argentinean, Colombian, Dominican, Nicaraguan, Salvadoran, Spaniard, and so on.* ↗

9. What is Person 1's race? Mark ☒ one or more boxes.

- ☐ White
- ☐ Black, African Am., or Negro
- ☐ American Indian or Alaska Native — *Print name of enrolled or principal tribe.* ↗

- ☐ Asian Indian
- ☐ Chinese
- ☐ Filipino
- ☐ Other Asian — *Print race, for example, Hmong, Laotian, Thai, Pakistani, Cambodian, and so on.* ↗
- ☐ Japanese
- ☐ Korean
- ☐ Vietnamese
- ☐ Native Hawaiian
- ☐ Guamanian or Chamorro
- ☐ Samoan
- ☐ Other Pacific Islander — *Print race, for example, Fijian, Tongan, and so on.* ↗

- ☐ Some other race — *Print race.* ↗

10. Does Person 1 sometimes live or stay somewhere else?

- ☐ No ☐ Yes — Mark ☒ all that apply.

- ☐ In college housing
- ☐ In the military
- ☐ At a seasonal or second residence
- ☐ For child custody
- ☐ In jail or prison
- ☐ In a nursing home
- ☐ For another reason

→ If more people were counted in Question 1, continue with Person 2.

1. Print name of Person 2

Last Name

First Name

MI

2. How is this person related to Person 1? Mark ☒ ONE box.

- | | |
|---|--|
| ☐ Husband or wife | ☐ Parent-in-law |
| ☐ Biological son or daughter | ☐ Son-in-law or daughter-in-law |
| ☐ Adopted son or daughter | ☐ Other relative |
| ☐ Stepson or stepdaughter | ☐ Roomer or boarder |
| ☐ Brother or sister | ☐ Housemate or roommate |
| ☐ Father or mother | ☐ Unmarried partner |
| ☐ Grandchild | ☐ Other nonrelative |

3. What is this person's sex? Mark ☒ ONE box.

- ☐ Male ☐ Female

4. What is this person's age and what is this person's date of birth?

Please report babies as age 0 when the child is less than 1 year old.

Print numbers in boxes.

Age on April 1, 2010 Month Day Year of birth

→ NOTE: Please answer BOTH Question 5 about Hispanic origin and Question 6 about race. For this census, Hispanic origins are not races.

5. Is this person of Hispanic, Latino, or Spanish origin?

- ☐ No, not of Hispanic, Latino, or Spanish origin
- ☐ Yes, Mexican, Mexican Am., Chicano
- ☐ Yes, Puerto Rican
- ☐ Yes, Cuban
- ☐ Yes, another Hispanic, Latino, or Spanish origin — Print origin, for example, Argentinean, Colombian, Dominican, Nicaraguan, Salvadoran, Spaniard, and so on. ↗

6. What is this person's race? Mark ☒ one or more boxes.

- ☐ White
- ☐ Black, African Am., or Negro
- ☐ American Indian or Alaska Native — Print name of enrolled or principal tribe. ↗

- | | | |
|--|-------------------------------------|--|
| ☐ Asian Indian | ☐ Japanese | ☐ Native Hawaiian |
| ☐ Chinese | ☐ Korean | ☐ Guamanian or Chamorro |
| ☐ Filipino | ☐ Vietnamese | ☐ Samoan |
| ☐ Other Asian — Print race, for example, Hmong, Laotian, Thai, Pakistani, Cambodian, and so on. ↗ | | |
| ☐ Other Pacific Islander — Print race, for example, Fijian, Tongan, and so on. ↗ | | |

- ☐ Some other race — Print race. ↗

7. Does this person sometimes live or stay somewhere else?

- ☐ No ☐ Yes — Mark ☒ all that apply.
- | | |
|--|---|
| ☐ In college housing | ☐ For child custody |
| ☐ In the military | ☐ In jail or prison |
| ☐ At a seasonal or second residence | ☐ In a nursing home |
| | ☐ For another reason |

→ If more people were counted in Question 1 on the front page, continue with Person 3.

1. Print name of Person 3

Last Name

First Name

MI

2. How is this person related to Person 1? Mark ☒ ONE box.

- | | |
|---|--|
| ☐ Husband or wife | ☐ Parent-in-law |
| ☐ Biological son or daughter | ☐ Son-in-law or daughter-in-law |
| ☐ Adopted son or daughter | ☐ Other relative |
| ☐ Stepson or stepdaughter | ☐ Roomer or boarder |
| ☐ Brother or sister | ☐ Housemate or roommate |
| ☐ Father or mother | ☐ Unmarried partner |
| ☐ Grandchild | ☐ Other nonrelative |

3. What is this person's sex? Mark ☒ ONE box.

- ☐ Male ☐ Female

4. What is this person's age and what is this person's date of birth?

Please report babies as age 0 when the child is less than 1 year old.

Print numbers in boxes.

Age on April 1, 2010 Month Day Year of birth

→ NOTE: Please answer BOTH Question 5 about Hispanic origin and Question 6 about race. For this census, Hispanic origins are not races.

5. Is this person of Hispanic, Latino, or Spanish origin?

- ☐ No, not of Hispanic, Latino, or Spanish origin
- ☐ Yes, Mexican, Mexican Am., Chicano
- ☐ Yes, Puerto Rican
- ☐ Yes, Cuban
- ☐ Yes, another Hispanic, Latino, or Spanish origin — Print origin, for example, Argentinean, Colombian, Dominican, Nicaraguan, Salvadoran, Spaniard, and so on. ↗

6. What is this person's race? Mark ☒ one or more boxes.

- ☐ White
- ☐ Black, African Am., or Negro
- ☐ American Indian or Alaska Native — Print name of enrolled or principal tribe. ↗

- | | | |
|--|-------------------------------------|--|
| ☐ Asian Indian | ☐ Japanese | ☐ Native Hawaiian |
| ☐ Chinese | ☐ Korean | ☐ Guamanian or Chamorro |
| ☐ Filipino | ☐ Vietnamese | ☐ Samoan |
| ☐ Other Asian — Print race, for example, Hmong, Laotian, Thai, Pakistani, Cambodian, and so on. ↗ | | |
| ☐ Other Pacific Islander — Print race, for example, Fijian, Tongan, and so on. ↗ | | |

- ☐ Some other race — Print race. ↗

7. Does this person sometimes live or stay somewhere else?

- ☐ No ☐ Yes — Mark ☒ all that apply.
- | | |
|--|---|
| ☐ In college housing | ☐ For child custody |
| ☐ In the military | ☐ In jail or prison |
| ☐ At a seasonal or second residence | ☐ In a nursing home |
| | ☐ For another reason |

→ If more people were counted in Question 1 on the front page, continue with Person 4.

1. Print name of **Person 4**

Last Name

First Name MI

2. How is this person related to Person 1? Mark ☒ ONE box.

- ☐ Husband or wife
- ☐ Parent-in-law
- ☐ Biological son or daughter
- ☐ Son-in-law or daughter-in-law
- ☐ Adopted son or daughter
- ☐ Other relative
- ☐ Stepson or stepdaughter
- ☐ Roomer or boarder
- ☐ Brother or sister
- ☐ Housemate or roommate
- ☐ Father or mother
- ☐ Unmarried partner
- ☐ Grandchild
- ☐ Other nonrelative

3. What is this person's sex? Mark ☒ ONE box.

- ☐ Male
- ☐ Female

4. What is this person's age and what is this person's date of birth?

Please report babies as age 0 when the child is less than 1 year old.
Print numbers in boxes.

Age on April 1, 2010

Month

Day

Year of birth

→ NOTE: Please answer BOTH Question 5 about Hispanic origin and Question 6 about race. For this census, Hispanic origins are not races.

5. Is this person of Hispanic, Latino, or Spanish origin?

- ☐ No, not of Hispanic, Latino, or Spanish origin
- ☐ Yes, Mexican, Mexican Am., Chicano
- ☐ Yes, Puerto Rican
- ☐ Yes, Cuban
- ☐ Yes, another Hispanic, Latino, or Spanish origin — Print origin, for example, Argentinean, Colombian, Dominican, Nicaraguan, Salvadoran, Spaniard, and so on.

6. What is this person's race? Mark ☒ one or more boxes.

- ☐ White
- ☐ Black, African Am., or Negro
- ☐ American Indian or Alaska Native — Print name of enrolled or principal tribe.

- ☐ Asian Indian
- ☐ Japanese
- ☐ Native Hawaiian
- ☐ Chinese
- ☐ Korean
- ☐ Guamanian or Chamorro
- ☐ Filipino
- ☐ Vietnamese
- ☐ Samoan
- ☐ Other Asian — Print race, for example, Hmong, Laotian, Thai, Pakistani, Cambodian, and so on.
- ☐ Other Pacific Islander — Print race, for example, Fijian, Tongan, and so on.

- ☐ Some other race — Print race.

7. Does this person sometimes live or stay somewhere else?

- ☐ No
- ☐ Yes — Mark ☒ all that apply.
- ☐ In college housing
- ☐ For child custody
- ☐ In the military
- ☐ In jail or prison
- ☐ At a seasonal or second residence
- ☐ In a nursing home
- ☐ For another reason

→ If more people were counted in Question 1 on the front page, continue with Person 5.

1. Print name of **Person 5**

Last Name

First Name MI

2. How is this person related to Person 1? Mark ☒ ONE box.

- ☐ Husband or wife
- ☐ Parent-in-law
- ☐ Biological son or daughter
- ☐ Son-in-law or daughter-in-law
- ☐ Adopted son or daughter
- ☐ Other relative
- ☐ Stepson or stepdaughter
- ☐ Roomer or boarder
- ☐ Brother or sister
- ☐ Housemate or roommate
- ☐ Father or mother
- ☐ Unmarried partner
- ☐ Grandchild
- ☐ Other nonrelative

3. What is this person's sex? Mark ☒ ONE box.

- ☐ Male
- ☐ Female

4. What is this person's age and what is this person's date of birth?

Please report babies as age 0 when the child is less than 1 year old.
Print numbers in boxes.

Age on April 1, 2010

Month

Day

Year of birth

→ NOTE: Please answer BOTH Question 5 about Hispanic origin and Question 6 about race. For this census, Hispanic origins are not races.

5. Is this person of Hispanic, Latino, or Spanish origin?

- ☐ No, not of Hispanic, Latino, or Spanish origin
- ☐ Yes, Mexican, Mexican Am., Chicano
- ☐ Yes, Puerto Rican
- ☐ Yes, Cuban
- ☐ Yes, another Hispanic, Latino, or Spanish origin — Print origin, for example, Argentinean, Colombian, Dominican, Nicaraguan, Salvadoran, Spaniard, and so on.

6. What is this person's race? Mark ☒ one or more boxes.

- ☐ White
- ☐ Black, African Am., or Negro
- ☐ American Indian or Alaska Native — Print name of enrolled or principal tribe.

- ☐ Asian Indian
- ☐ Japanese
- ☐ Native Hawaiian
- ☐ Chinese
- ☐ Korean
- ☐ Guamanian or Chamorro
- ☐ Filipino
- ☐ Vietnamese
- ☐ Samoan
- ☐ Other Asian — Print race, for example, Hmong, Laotian, Thai, Pakistani, Cambodian, and so on.
- ☐ Other Pacific Islander — Print race, for example, Fijian, Tongan, and so on.

- ☐ Some other race — Print race.

7. Does this person sometimes live or stay somewhere else?

- ☐ No
- ☐ Yes — Mark ☒ all that apply.
- ☐ In college housing
- ☐ For child custody
- ☐ In the military
- ☐ In jail or prison
- ☐ At a seasonal or second residence
- ☐ In a nursing home
- ☐ For another reason

→ If more people were counted in Question 1 on the front page, continue with Person 6.

1. Print name of **Person 6**

Last Name

First Name MI

2. How is this person related to Person 1? Mark ☒ ONE box.

- | | |
|---|--|
| ☐ Husband or wife | ☐ Parent-in-law |
| ☐ Biological son or daughter | ☐ Son-in-law or daughter-in-law |
| ☐ Adopted son or daughter | ☐ Other relative |
| ☐ Stepson or stepdaughter | ☐ Roomer or boarder |
| ☐ Brother or sister | ☐ Housemate or roommate |
| ☐ Father or mother | ☐ Unmarried partner |
| ☐ Grandchild | ☐ Other nonrelative |

3. What is this person's sex? Mark ☒ ONE box.

- ☐ Male ☐ Female

4. What is this person's age and what is this person's date of birth?

Please report babies as age 0 when the child is less than 1 year old.
Print numbers in boxes.

Age on April 1, 2010 Month Day Year of birth

→ NOTE: Please answer BOTH Question 5 about Hispanic origin and Question 6 about race. For this census, Hispanic origins are not races.

5. Is this person of Hispanic, Latino, or Spanish origin?

- ☐ No, not of Hispanic, Latino, or Spanish origin
- ☐ Yes, Mexican, Mexican Am., Chicano
- ☐ Yes, Puerto Rican
- ☐ Yes, Cuban
- ☐ Yes, another Hispanic, Latino, or Spanish origin — Print origin, for example, Argentinean, Colombian, Dominican, Nicaraguan, Salvadoran, Spaniard, and so on. ↴

6. What is this person's race? Mark ☒ one or more boxes.

- ☐ White
- ☐ Black, African Am., or Negro
- ☐ American Indian or Alaska Native — Print name of enrolled or principal tribe. ↴

- | | | |
|--|---|--|
| ☐ Asian Indian | ☐ Japanese | ☐ Native Hawaiian |
| ☐ Chinese | ☒ Korean | ☐ Guamanian or Chamorro |
| ☐ Filipino | ☐ Vietnamese | ☐ Samoan |
| ☐ Other Asian — Print race, for example, Hmong, Laotian, Thai, Pakistani, Cambodian, and so on. ↴ | ☐ Other Pacific Islander — Print race, for example, Fijian, Tongan, and so on. ↴ | |

- ☐ Some other race — Print race. ↴

7. Does this person sometimes live or stay somewhere else?

- ☐ No ☐ Yes — Mark ☒ all that apply.
- | | |
|--|---|
| ☐ In college housing | ☐ For child custody |
| ☐ In the military | ☐ In jail or prison |
| ☐ At a seasonal or second residence | ☐ In a nursing home |
| | ☐ For another reason |

→ If more than six people were counted in Question 1 on the front page, turn the page and continue.

INTERNATIONAL COPY

→ If more people live here, turn the page and continue.

Use this section to complete information for the rest of the people you counted in Question 1 on the front page. We may call for additional information about them.

Person 7

Last Name

First Name

MI

Sex

Age on April 1, 2010

Date of Birth

Related to Person 1?

☐ Male
☐ Female

Month Day Year

☐ Yes
☐ No

Person 8

Last Name

First Name

MI

Sex

Age on April 1, 2010

Date of Birth

Related to Person 1?

☐ Male
☐ Female

Month Day Year

☐ Yes
☐ No

Person 9

Last Name

First Name

MI

Sex

Age on April 1, 2010

Date of Birth

Related to Person 1?

☐ Male
☐ Female

Month Day Year

☐ Yes
☐ No

Person 10

Last Name

First Name

MI

Sex

Age on April 1, 2010

Date of Birth

Related to Person 1?

☐ Male
☐ Female

Month Day Year

☐ Yes
☐ No

Person 11

Last Name

First Name

MI

Sex

Age on April 1, 2010

Date of Birth

Related to Person 1?

☐ Male
☐ Female

Month Day Year

☐ Yes
☐ No

Person 12

Last Name

First Name

MI

Sex

Age on April 1, 2010

Date of Birth

Related to Person 1?

☐ Male
☐ Female

Month Day Year

☐ Yes
☐ No

**Thank you for completing your official
2010 Census form.**

FOR OFFICIAL USE ONLY

JIC1

JIC2

If your enclosed postage-paid envelope is missing, please mail your completed form to:

**U.S. Census Bureau
National Processing Center
1201 East 10th Street
Jeffersonville, IN 47132**

If you need help completing this form, call 1-866-872-6868 between 8:00 a.m. and 9:00 p.m., 7 days a week. The telephone call is free.

TDD — Telephone display device for the hearing impaired. Call 1-866-783-2010 between 8:00 a.m. and 9:00 p.m., 7 days a week. The telephone call is free.

¿NECESITA AYUDA? Si usted necesita ayuda para completar este cuestionario, llame al 1-866-928-2010 entre las 8:00 a.m. y 9:00 p.m., 7 días a la semana. La llamada telefónica es gratis.

The U.S. Census Bureau estimates that, for the average household, this form will take about 10 minutes to complete, including the time for reviewing the instructions and answers. Send comments regarding this burden estimate or any other aspect of this burden to: Paperwork Reduction Project 0607-0919-C, U.S. Census Bureau, AMSD-3K138, 4600 Silver Hill Road, Washington, DC 20233. You may e-mail comments to <Paperwork@census.gov>; use "Paperwork Project 0607-0919-C" as the subject.

Respondents are not required to respond to any information collection unless it displays a valid approval number from the Office of Management and Budget.

Exhibit 17

<http://www.osec.doc.gov/opog/privacy/Census-pias.html>

Go

JAN FEB MAY

02

2016 2017 2018

About this

4 captures

2 Feb 2017 - 26 Jun 2017

HOME

PRIVACY

OPEN GOVERNMENT

FOIA

PRIVACY ACT

FACA

DIRECTIVES

ABOUT

CONTACT US

U.S. Census Bureau

Privacy Impact Assessments (PIAs) and Privacy Threshold Analysis (PTA)

System Name	PTA	PIA	Approval Date
• CEN01 Data Communications		PIA	4/23/2015
• CEN02 Lenel		PIA	8/8/2016
• CEN03 Economic Census and Surveys and Special Processing		PIA	6/28/2016
• CEN04 Commerce Business Systems		PIA	3/4/2015
• CEN05 Field Systems Major Application System		PIA	6/29/2015
• CEN06 National Processing Center (NPC)		PIA	8/20/2014
• CEN08 Decennial		PIA	8/11/2014
• CEN09 Cloud Services		PIA	10/16/2016
• CEN11 Demographic Census, Surveys, and Special Processing		PIA	7/1/2014
• CEN12 AESDirect		PIA	9/17/2014
• CEN13 Center for Economic Studies		PIA	6/2/2015

<http://www.osec.doc.gov/opog/privacy/Census-pias.html>

Go

JAN FEB MAY



9/17/2014

4 captures

2 Feb 2017 - 26 Jun 2017

2016 2017 2018

About this capture

- CEN15 Centurion [PIA](#) 2/10/2015
- CEN17 Client Services General Support System [PIA](#) 8/8/2016
- CEN18 Enterprise Applications [PIA](#) 6/7/2016
- CEN20 Budget Division Applications [PIA](#) 5/5/2016
- CEN21 Human Resources Division Applications [PIA](#) 8/8/2016
- CEN25 Office of Information Security (OIS) Systems [PIA](#) 10/1/2014
- CEN26 SharePoint [PIA](#) 7/16/2015
- CEN30 Amercian Community Survey [PIA](#) 3/24/2015
- CEN31 Administrative Systems Vol. II [PIA](#) 4/27/2016
- CEN33 DataWeb [PIA](#) 2/4/2015
- CEN34 Foreign Trade Division Applications [PIA](#) 6/2/2014
- CEN35 Governments Division Applications [PIA](#) 11/4/2014
- CEN36 integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), and MOJO Enhanced Operational Control System [PIA](#) 7/15/2015
- Automated Export System (AES) [PIA](#) 8/11/2014

<http://www.osec.doc.gov/opog/privacy/Census-pias.html>

Go

JAN FEB MAY



Customer Experience Management (CEM) Pilot

02 PIA

4/23/2015

4 captures

Project

2 Feb 2017 - 26 Jan 2017

2016 2017 2018

About this capture

- Social Media and Web 2.0 Websites and Applications (Third Party Website with PII)

[PIA](#)

3/31/2015

Questions and Comments

Send Questions, Comments or Complaints on the Commerce Privacy program to CPO@doc.gov.

Office of Privacy and Open Government
Office of the Chief Financial Officer and Assistant Secretary for Administration
U.S. Department of Commerce

Page last updated: December 13, 2016

Exhibit 18

BYLAWS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER ("EPIC")

As Adopted As of March 16, 2000,
As Amended May 1, 2007,
As Amended February 8, 2010,
As Amended February 1, 2015,
As Amended January 26, 2018

ARTICLE I
NAME AND PURPOSES

Section 1.01. Name. The name of the organization is ELECTRONIC PRIVACY INFORMATION CENTER.

Section 1.02. Purpose. The Corporation is organized for the charitable and educational purposes of promoting personal privacy and constitutional rights.

ARTICLE II
AUTHORITY AND DUTIES OF DIRECTORS

Section 2.01. Authority of Directors. The Board of Directors ("the Board") is the policy-making body and may exercise all the powers and authority granted to the Corporation by law.

Section 2.02. Number, Selection, and Tenure. The Board shall consist of no more than fifteen (15) nor less than seven (7) Directors, all of whom must be Members of the Corporation, elected in staggered terms of three (3) years, nominated from among its Members, and confirmed by the Board. A director may serve for any number of terms, consecutive or otherwise. Directors will be elected by the directors then in office. The Board will seek to promote pluralism and diversity among its membership.

Section 2.03. Compensation. Board members shall not be compensated for serving on the Board, but may be reimbursed for actual expenses incurred on behalf of the Corporation. Board members who also serve as employees of the Corporation may be compensated for their service as employees. No more than one (1) paid staff member shall serve as a voting member of the Board. A paid staff member serving on the Board shall not serve as the Chair or Treasurer.

Section 2.04. Resignation and Removal. Resignations are effective upon receipt by the Secretary of written notification, or receipt by the President or other officer if the Secretary is resigning. One or more Directors may be removed at a meeting called for that purpose, with or without cause, by such vote as would suffice for the Director's election.

Section 2.05. Vacancies. Vacancies existing by reason of resignation, death, incapacity or removal before the expiration of a term shall be filled by a majority vote of the remaining

directors.

Section 2.06. Meetings. The Board shall hold at least one regular meeting annually. Regular meetings shall be at such times and places as the Board shall determine. Special meetings may be called by any two directors with telephone or written notice.

If an officer or director fails to attend three (3) consecutive meetings of the Board or Executive Committee, the Executive Committee shall evaluate the officer's or director's contribution to the work of the Corporation, his or her reasons for not attending the meetings, as well as any other relevant factors, and if it appears to be in the best interest of the Corporation, may declare the position vacant.

Section 2.07. Quorum and Voting. A quorum shall consist of a majority of the total number of Board members in office. All decisions will be by majority vote of those present at a meeting at which a quorum is present.

Section 2.08. Action Without a Meeting. Any action required or permitted to be taken at a meeting of the Board (including amendment of these Bylaws or the Articles of Incorporation) or of any committee may be taken without a meeting if all the members of the Board or committee consent in writing to taking the action without a meeting and to approving the specific action. Such consents shall have the same force and effect as a unanimous vote of the Board or of the committee as the case may be.

Section 2.09. Participation in Meeting by Conference Telephone. Any or all members of the Board may participate in a meeting by conference telephone or similar communications equipment, so long as members participating in such meeting can hear one another.

Section 2.10. Committees. The Board may, by resolution adopted by a majority of the Directors in office, establish committees of the Board composed of at least two (2) Directors.

Other committees not having and exercising the authority of the Board in the management of the corporation may be designated and appointed by a resolution adopted by a majority of the directors present at a meeting at which a quorum is present. Such committees shall consist of at least two members.

The standing committees of the Board shall be an Executive Committee, composed of the officers, and the Program and Litigation Committee, Finances and Fundraising Committee, Management and Staffing Committee, and Engagement and Outreach Committee. The names of these committees may be changed by resolution of the Board.

For both types of committees, the Board may make provisions for appointment of the chair, establish procedures to govern their activities, and delegate authority as may be necessary or desirable for the efficient management of the property, affairs, business, and/or activities of the Corporation.

ARTICLE III
AUTHORITY AND DUTIES OF OFFICERS

Section 3.01. Officers. The officers of the Corporation shall be a President, a Chair, a Secretary, a Treasurer, and such other officers as the Board may designate. Two or more offices may be held by the same person, except the offices of secretary and president.

Section 3.02. Election of Officers; Terms of Office. Officers shall serve one (1) year terms. The President, the Secretary, and the Treasurer shall be elected by the Board at its annual meeting in each year. The terms of office shall expire at the next succeeding annual meeting and shall be filled by the Board, at a meeting or by action in writing pursuant to Section 2.08 for a term expiring at the next succeeding annual meeting. Officers shall be eligible for reelection.

Vacancies existing by reason of resignation, death, incapacity or removal before the expiration of a term shall be filled by the Board for the remainder of the unexpired term.

Section 3.03. Resignation. Resignations are effective upon receipt by the Secretary of a written notification, or receipt by the President if the Secretary is resigning.

Section 3.04. Removal. An officer may be removed by the Board at a meeting, or by action in writing pursuant to Section 2.08 whenever in the Board's judgment the best interests of the Corporation will be served thereby. The removal of a person from corporate office will not terminate or otherwise affect any contractual relationship between that individual and the corporation.

ARTICLE IV
INDEMNIFICATION

Section 4.01. Definitions. "Matter" shall mean any actual or threatened civil, criminal, or administrative action, arbitration proceeding, claim, suit, proceeding, or appeals therefrom, or any criminal, administrative, or Congressional (or other body's) investigation, hearing, or other proceeding.

"Eligible Person" shall mean any person who at any time was or is a director, a member or any committee or subcommittee, an officer, employee, or volunteer of the corporation.

Section 4.02. Right to Indemnification. Any Eligible Person made a party to or involved in a Matter by reason of his or her position with or service to the corporation shall, to the fullest extent permitted by law, be indemnified by the corporation against all liabilities and all expenses reasonably incurred by him or her arising out of or in connection with such Matter, except in relation to Matters as to which (i) the Eligible Person failed to act in good faith and for a purpose which he or she reasonably believed to be in the best interests of the corporation, or (ii) in the case of a criminal Matter, the person had reasonable cause to believe that his or her conduct was unlawful, or (iii) the person shall be adjudged to be liable for willful misconduct in the performance of a duty, or in the case of a Matter settled by agreement, the settlement shall be predicated on such a liability.

Section 4.03. Limitation on Right of Indemnification. Except where an Eligible Person has been successful on the merits with respect to such Matter, any indemnification hereunder shall be made only after (i) the Board (acting by a quorum consisting of Directors who were not involved in such Matter) determines that the Eligible Person met the applicable indemnification standard set forth in section 4.02 above; or (ii) in the absence of a quorum, a finding is rendered in a written opinion by independent legal counsel that the person or persons met the applicable indemnification standard set forth in section 4.02 above.

Section 4.04. Other Rights. The right of indemnification provided hereunder shall not be deemed exclusive of any other right to which any person may be entitled in addition to the indemnification provided hereunder. This indemnification shall in the case of the death of the person entitled to indemnification, inure to the benefit of his or her heirs, executors or other lawful representative.

Section 4.05. Interim Indemnification. The corporation shall, with respect to a Matter described in section 4.02, advance attorneys fees as interim indemnification to any Eligible Person if the following conditions are satisfied: (i)(a) the Board (acting by a quorum consisting of Directors who are not involved in such litigation) determines that the Eligible Person is likely to meet the applicable indemnification standard set forth in section 4.02 above, or (b) in the absence of such a quorum, a finding is rendered in a written opinion by independent legal counsel that the Eligible Person is likely to meet the applicable indemnification standard set forth in section 4.02 above; and (ii) the Eligible Person (a) requests interim indemnification, (b) agrees to repay the interim indemnification promptly upon a determination unfavorable to him or her under section 4.03, and (c) deposits a bond or equivalent security.

Section 4.06. Insurance. The Board may authorize the purchase of and maintain insurance on behalf of any Eligible Person against any liability asserted against or incurred by him which arises out of such person's status in such capacity, or out of acts taken in such capacity, whether or not the Corporation would have the power to indemnify the person against that liability under law.

ARTICLE V MEMBERS

Section 5.01. Qualifications. The Corporation shall designate as Members, following nomination by the current Members and a vote of the Board, distinguished experts in law, technology, and public policy.

Section 5.02. Advisory Board. Members shall sit on the Advisory Board, where they shall provide guidance for the work of the Corporation, participate in the activities of the Corporation, offer support for the Corporation, and provide leadership for the Corporation

Section 5.03. Dues. Members shall pay dues in an amount and on a schedule established by the Board. There shall be provisions for lifetime memberships.

Section 5.04. Service on Committees. Members may serve on Board committees.

Section 5.05. Annual Meeting. There shall be an annual meeting, open to all Members of the Corporation.

Section 5.05. Annual Evaluation. The Members shall provide an annual evaluation of the Corporation, which shall be reported to the Board of Directors at the Annual Meeting.

ARTICLE VI FINANCIAL ADMINISTRATION

Section 6.01. Fiscal Year. The fiscal year of the Corporation shall be January 1 -December 31 but may be changed by resolution of the Board.

Section 6.02. Checks, Drafts, Etc. All checks, orders for the payment of money, and insurance certificates shall be signed or endorsed by an officer or officers or agent or agents of the Corporation and in a manner as shall from time to time be determined by resolution of the Board or of any committee to which such authority has been expressly delegated by the Board.

Section 6.03. Contracts. Unless the Board determines otherwise by resolution, the President, Secretary, Treasurer, Board Chair and Chair of the Executive Committee shall all be authorized to execute contracts on behalf of the corporation.

These individuals may, with written notice to the Board, delegate this authority to employees or volunteers subject to limitations upon the delegated authority as may be necessary or expedient for running the affairs of the corporation. Unless otherwise expressly determined by the Board, no other individuals shall be authorized to bind the corporation to any contract, including the chair of any committee other than the Executive Committee.

Section 6.04. Deposits and Accounts. All funds of the Corporation, not otherwise employed, shall be deposited in general or special accounts in the banks, trust companies, or other depositories as the Board or any committee to which such authority has been delegated by the Board may select, or as may be selected by any officer or officers or agent or agents of the Corporation, to whom such power may be delegated by the Board. For the purpose of deposit and for the purpose of collection for that account of the Corporation, checks, drafts, and other orders of the Corporation may be endorsed, assigned, and delivered on behalf of the Corporation by any officer or agent of the Corporation.

Section 6.05. Annual Financial Statements. Complete financial statements shall be presented to and reviewed by the Board after the close of each fiscal year.

ARTICLE VII CONFLICTS OF INTEREST

Section 7.01. Disclosure of Financial Interests. To identify possible conflicts of interest, all directors, officers, and members of any committee exercising Board- delegated powers must

disclose to the Board, or to the members of such committee, the existence of any financial interest in any entity with which s/he knows or has reason to know the Corporation or any legally related organization has or is negotiating a transaction or arrangement, and all material facts related to that interest. Financial interests include any direct or indirect relationship, through business, investment, or family, such as actual or potential ownership or investment interests or compensation arrangements. Directors shall also disclose any fiduciary duty to a person or entity other than the Corporation that might jeopardize the director's ability to exercise independent judgment and act in the best interests of the Corporation. The fact that a director, officer, or committee member is also a director or officer or member of a not-for-profit organization that obtains or seeks funds from institutions or individuals from which the Corporation also obtains or seeks funds shall not by itself be deemed to be a conflict of interest.

Section 7.02. Determination of Conflicts of Interest. After the interested person has delivered all relevant information and has retired from the room, the Board or committee must determine whether or not the financial interest creates a conflict of interest that merits recusal of the interested Director from consideration of the matter.

Section 7.03. Resolution of Conflicts of Interest. If the Board determines that a conflict of interest does exist, it must ensure that the interested director(s) do not participate in final decision making with regard to the transaction. The Board may approve the transaction or arrangement, or some alternative if it determines it: a) is in the organization's best interests and for its own benefit; b) is fair and reasonable to the organization; and c) is the most advantageous transaction or arrangement the organization can obtain with reasonable efforts under the circumstances.

Section 7.04. Violation of Conflict of Interest Policy. If an officer, director, or member of a committee with Board-delegated powers violates this conflict of interest policy, the Board, in order to protect the Corporation's best interests, may take appropriate disciplinary action against the interested person. Such action may include formal reprimand, cancellation of the transaction or arrangement generating the conflict, suspension of employment, and/or removal from the Board.

Section 7.05. Distribution of Conflict of Interest Policy. All officers, directors, and members of committees with Board-delegated powers shall receive a copy of the Conflict of Interest Policy, as it appears in these By-laws. All officers, directors, and members of committees with Board-delegated powers shall sign an annual statement declaring that the person: received a copy of the policy; has read and understands the policy; and agrees to comply with the policy.

ARTICLE VIII COMPENSATION

The Board shall adopt a policy establishing procedures for reviewing and setting financial compensation to any individual exercising substantial influence over the corporation to ensure that such compensation is no more than reasonable and does not otherwise result in an excess benefit to the person, and requiring that adequate documentation be maintained to support the basis for setting such compensation.

ARTICLE IX
RECORD KEEPING

The Secretary or his or her designee shall keep or cause to be kept adequate minutes of all Board or committee meetings, and all meetings of committees with Board-designated powers reflecting at a minimum the names of those in attendance, any resolutions passed and the outcomes of any votes taken. When potential conflicts of interests are discussed, the minutes shall include: the names of the persons who disclosed financial interests; the nature of the financial interests; whether or not the Board determined that a conflict existed; the names of the persons present for the discussions and votes related to the relevant transaction or arrangement; the content of those discussions, including any alternative transactions or arrangements; and a record of the vote. At the request of any participating Board member, the records of such discussions and individual votes may be kept sealed, with only the outcome reported publicly.

ARTICLE X
ANNUAL REPORTS

An annually updated written account of the Corporation's purposes, structure, programs and financial condition shall be published and made publicly available. The annual report shall contain: a description of the Corporation's purpose(s); descriptions of its overall programs, activities and accomplishments; a statement of its eligibility to receive deductible contributions; information about the governing body and structure, including identification of officers, directors, and chief administrative personnel; and the audited financial statements or, at a minimum, a comprehensive financial summary that reflects all revenue, reports expenses by program, management and fund-raising categories, and reports year-end balances.

ARTICLE XI
AMENDMENT OF BYLAWS

These Bylaws may be amended by a majority vote of the Board, provided seven (7) days' prior notice is given of the proposed amendment or provided all members of the Board waive such notice, or by unanimous consent in writing without a meeting pursuant to Section 2.08.

Exhibit 19

PREPARED STATEMENT OF
RON JARMIN, PhD.
PERFORMING THE NON-EXCLUSIVE FUNCTIONS AND DUTIES OF
THE DIRECTOR
U.S. CENSUS BUREAU

and

EARL COMSTOCK
DIRECTOR, OFFICE OF POLICY AND STRATEGIC PLANNING
U.S. DEPARTMENT OF COMMERCE

Before the Committee on Oversight and Government Reform
U.S. House of Representatives

“Progress Report on the 2020 Census”

8 May 2018

Good afternoon, Chairman Gowdy, Ranking Member Cummings, and members of the Committee. We welcome this opportunity to update you on the status of the 2020 Census. Before we begin, we would like to thank Congress for the Census Bureau’s recent appropriation, which underscores Congress’ commitment to a successful 2020 Census. The Department of Commerce and Census Bureau share your commitment and today we will provide a brief review of our progress to conduct a complete and accurate census.

2018 End-to-End Census Test

We are in the midst of the 2018 End-to-End Census Test. This is our final major field test before the 2020 Census. We are testing the interfaces between 44 IT systems critical for the 2020 Census, and their integration with the 24 major operations that are part of the 2018 End-to-End Census Test.

Tomorrow, we begin the Nonresponse Follow-up Operations for the 2018 End-to-End Census Test. Nonresponse Follow-up is an eight-week field operation to gather responses from households that have not yet responded by Internet, telephone, or paper questionnaire. Approximately 56 percent of households in the test did not respond to the Census questionnaire, so we will send approximately 900 enumerators to knock on doors and gather the information. This key operation involves 31 systems with appropriate interfaces, and will provide important feedback as we prepare to conduct the 2020 Census.

The 2018 End-to-End Census Test's Nonresponse Follow-up operation began in August 2017 with the Address Canvassing operation in three locations: Pierce County, Washington; the Bluefield-Beckley-Oak Hill, West Virginia area; and, Providence County, Rhode Island. These locations allowed the Census Bureau to test systems with and without Internet connectivity and to study critical address list development operations in a wide range of geographical situations including rural and mountainous areas. Importantly, in areas with low Internet connectivity Census Bureau field staff were able to receive their assignments and submit their payroll and operational data at the beginning or end of their shifts. By design, staff began and ended their shifts in areas with Internet connectivity so that they could do this. They did not require Internet access while they were actually conducting the listing operation. We were able to successfully integrate with the operational control system in field conditions. We also integrated with the other decennial systems effectively, such as the system we are using to provide directional information to staff ensuring they complete their work in the most efficient manner possible. Additionally, we tested the implementation of the independent quality control component, which ensures the proper disposition of cases in real time providing us with important information when cases fail to pass quality control.

The 2017 Address Canvassing operation revealed areas where our systems and operations need to improve, especially with regard to training. Some of these areas are being addressed as we continue to refine our training modules. Address listing is a complicated process and we have identified ways to improve technical training. The West Virginia site, in particular, experienced connectivity issues. The challenge of unreliable wireless signals is one of the reasons that site was chosen. Because of connectivity issues, some of the employees hired to carry out the address listing operation had difficulty completing the self-paced online training at their home. We continue to examine the experiences of our listers so that we can enhance this functionality and improve both systems and operations.

Just as we learned a great deal from the Address Canvassing operation, we are learning from the operations conducted in Providence. We will continue to make the necessary adjustments to our systems and operations in response to what we observe and experience during the 2018 End-to-End Census Test.

We opted to conduct the 2018 End-to-End Test in Providence County because it represents an ideal location for testing data collection operations. It offers many different situations and provides challenges that we will face across the country in 2020, and its demographics mirror those of the nation. Providence County has a population of over 600,000, more than a quarter-million housing units, and historically hard-to-count populations. Providence County provides an opportunity to test all of the systems and operations planned for the 2018 End-to-End Census Test. Providence County's urban areas include high vacancy rates, and neighborhoods and housing that have undergone considerable conversion for many years. This allows us to validate our address canvassing operation (for example, identifying split or converted housing units). There also is a solid presence of Group Quarters, which are residences that contain multiple unrelated residents, allowing us to conduct that operation.

The test's self-response phase began with a series of mailings that were sent to housing units beginning in mid-March. We received a high number of responses through the Internet—almost

64 percent of the total responses. Households also are responding by telephone (6 percent) or returning the paper questionnaire by mail (30 percent). However, consistent with our planned approach for the 2020 Census, households only received a questionnaire on the first mailing if the household does not have strong Internet connectivity or if the household is considered unlikely to use the Internet. Households with older people often fall into this latter category. Regardless, every household that had not responded after three mailings received a paper questionnaire on the fourth mailing.

The remaining peak operations in Providence, Rhode Island, are Group Quarters, Update Leave, and Nonresponse Follow-up. The Group Quarters operation is designed to enumerate people who live in places such as college dormitories, skilled nursing facilities, and prisons. The Update Leave operation is designed for areas that do not have a city-style address, such as “100 Main Street,” where the address and the geographic location of the housing units are linked. Areas without city-style addresses are most common in rural areas where mailing addresses are grouped together (e.g., multiple mail boxes grouped together at the end of a rural road) and not tied to the geographic location of the actual housing unit (e.g., Post Office Boxes). During Update Leave, field staff will update our address list and leave a questionnaire packet at each household in this area. Those who do not respond are included in the Nonresponse Follow-up operation where we collect information by sending a census enumerator to interview the household.

All of the planned innovations for the 2020 Census are coming together in the 2018 End-to-End Census Test and the lessons learned will provide a firm foundation for success in 2020. We are looking closely at data from the Address Canvassing operation to make sure that our blend of in-office and in-field Address Canvassing meets our standards for an accurate and comprehensive address list. The Internet and telephone response modes are being thoroughly tested, as is the Paper Data Capture operation. We also are making it easier for people to respond in real time with a smart phone or a tablet. Field staff will collect information using hand-held devices and their work will be managed efficiently and effectively by leveraging automated processes. Finally, we will continue to examine the use of administrative records to inform final determinations about our ability to improve the efficiency of the Nonresponse Follow-up operation using information that people have already provided to the government. During and after the test, we will adjust the systems and operations based on what we learned to make sure that both are ready for the 2020 Census.

Systems Readiness

We developed a comprehensive schedule for developing and integrating the key systems for the 2018 End-to-End Census Test. Each system has its own well-defined scope, requirements, schedule, and costs, and each is overseen by experienced project management teams. As we enter the peak operations of the test, 40 out of the 44 systems supporting the test have been deployed. No system will be released without completing the necessary integration testing and security authorizations. All 44 are on track to be fully integrated and deployed when they are needed to support operations in the test.

The Census Bureau has been working closely with the Government Accountability Office (GAO) to ensure that the Census Bureau and the GAO share a consistent understanding of the status of systems readiness, and we both are monitoring final development and testing of the remaining systems needed for the 2018 End-to-End Census Test. All of our systems for the 2020 Census are being integrated through a contracted solution that the Census Bureau refers to as the “technical integrator.”

The Census Bureau’s Office of Information Security, under the guidance of the Department of Commerce’s Chief Information Officer, is working with the technical integrator to ensure that the systems are secure and are authorized to operate (ATO) before going live. The ATO process is critical because it ensures that cybersecurity standards are addressed and risks are minimized for all systems based on federal policies and procedures. GAO is reviewing our progress to ensure that our processes and procedures within our Systems Engineering and Integration framework are consistent with GAO’s best practices. We value GAO’s independent assessment and are appreciative of their continued assessment and support.

With respect to the 2018 End-to-End Census Test and looking forward to the 2020 Census, the Census Bureau is maintaining a well-defined schedule and framework for releasing systems for the remainder of the 2018 Test and then for the 2020 Census. Lessons learned from the 2018 Test will be incorporated to enhance and improve the systems. We also have a well-developed process for conducting the scalability tests on our systems during 2018. The technical integrator is enabling the scalability test using infrastructure in the cloud and the data center. Conducting the scalability tests is a major milestone this year, and we are eager to meet this milestone and fine tune our systems to scale to predicted peak loads in 2020.

Finally, we are engaging with the private sector and the federal government intelligence community in the area of cybersecurity to ensure the information we collect is protected, that we can withstand the threat of cyber attacks, and, if necessary, contain a threat in a way that sustains service and maintains public trust.

2020 Operations Already Underway: LUCA, In-Office Address Canvassing, and Delivery of the 2020 Census Questions

Even as we are in the midst of the 2018 End-to-End Census Test, key operations for the 2020 Census are already up and running. Today, we would like to summarize our progress on the Local Update of Census Addresses (LUCA) program, In-Office Address Canvassing, and the delivery of the 2020 Census planned questions to Congress.

LUCA, which began last year, provides tribal, state, and local governments an opportunity to review and comment on the Census Bureau’s address list, while following the requirements of Title 13. More than eleven thousand governmental units, 45 states, the District of Columbia, and the Commonwealth of Puerto Rico, as well as major counties and cities, and tribal governments, have registered for the 2020 Census LUCA program. These registrations exceed those for the 2010 Census program and we are pleased that they cover more than 98 percent of both the country’s housing units and the population. The Census Bureau has begun sending these governments their address packages so that they can conduct their review. As of today,

approximately 1200 hundred governments have returned their packages to the Census Bureau, and of these about 30 percent of the submissions have not made any changes to the address list.

The In-Office Address Canvassing operation is one of the important innovations in the 2020 Census. Since 2015, we have been updating the most recent Census Bureau address list with new information from the United States Postal Service and data from tribal, state, and local governments and third parties (i.e., commercial vendors). We also review satellite imagery to help determine where address changes are occurring. Based on these changes, the Census Bureau will develop a plan for capturing those changes. This plan will include In-Field Address Canvassing where address updates cannot be obtained or verified or in areas undergoing rapid change. The number of addresses requiring In-Field Address Canvassing is expected to be approximately 30 percent of the total number of addresses, compared to 100 percent in 2010.

The Census Bureau is required by Section 141(f) of Title 13 of the U.S. Code to submit the subjects proposed for the next census to Congress no later than three years before April 1st of the upcoming decennial year. A document fulfilling that requirement was submitted to Congress on March 28, 2017. Section 141(f) also requires the questions proposed to be included in the next census be submitted to Congress no later than two years before Census Day, which will be April 1, 2020. The document that fulfilled this requirement for the 2020 Census, and the American Community Survey, was delivered to Congress on March 29, 2018. Pursuant to the Paperwork Reduction Act of 1995, later this year the Census Bureau will provide the public an opportunity to comment on the proposed questions, and then send the proposed questions to OMB.

As background, we would like to provide an overview of the process for determining the content on the 2020 Census and the American Community Survey. The Department of Commerce and the Census Bureau conduct a rigorous legal, technical, program, and policy review of each question to determine whether it should be included for the Decennial Census Program, which includes the 2020 Census and the American Community Survey. When it passed Title 13, Congress delegated to the Secretary of Commerce the authority to determine content for the Decennial Census Program.

Throughout each decade, regular content reviews are conducted to ensure that the information collected through the Decennial Census Program is required by federal programs. In December 2017, the Department of Justice requested that the Census Bureau reinstate a citizenship question on the 2020 Census to provide census block level citizenship voting age population data, which DOJ finds critical to its enforcement of Section 2 of the Voting Rights Act. This request underwent a thorough legal, technical, and policy review. On March 26, 2018, the Secretary of Commerce directed the Census Bureau to reinstate the citizenship question on the 2020 Census.

For the 2020 Census, the Census Bureau will use the citizenship question currently used on the American Community Survey. A question on citizenship has been asked on the American Community Survey each year since 2005 and also was asked on the long form censuses in 1970, 1980, 1990, and 2000.

The Census Bureau currently is taking steps to make the necessary operational adjustments to all data collection and processing systems to include the new question. The Census Bureau also is

taking steps to further enhance its administrative record data sets, protocols, and statistical models to provide more complete and accurate data. As is our standard practice, the Census Bureau will conduct research and develop this administrative records use strategy in an open and transparent manner, consulting with expert groups and stakeholders.

In addition to citizenship, the 2020 Census will ask questions about age, sex, race, Hispanic origin, relationship, and tenure. Some operational questions, such as name and telephone number, also are asked to better administer the data collection process and to ensure greater accuracy of the data collected. Contact information is not part of the published data and all data collected is carefully protected, as mandated by federal law, to maintain confidentiality and respect the personal information of respondents.

The document *Questions Planned for the 2020 Census and American Community Survey*, which was delivered to Congress on March 29, 2018, includes images of each question, information about why we ask each question, and the federal and selected local community uses of the data.

American Community Survey data are critical for communities and businesses nationwide. The American Community Survey is the nation's premier survey, providing the only source of comparable data for all of America's communities, and will continue to cover more than 35 topics, for example, school enrollment, veteran status and period of service, home value, and computer and Internet use. In 2019 and 2020, the Census Bureau will implement several changes to make it easier for respondents to answer the survey questions and improve the quality of the American Community Survey data.

The 2020 Census also is conducted in the Island Areas of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the U.S. Virgin Islands. For the 2020 Island Areas Censuses, we plan to use a modified version of the American Community Survey form that better meets the needs of the Island Areas. For example, we do not plan to ask about home heating fuel but do plan to ask about sewage disposal and source of water. This innovative approach of using existing data collection and processing systems will enable the Census Bureau to more quickly and efficiently tabulate and publish data from the 2020 Census for the Island Areas.

Enumerating Traditionally Undercounted Populations

To ensure a complete and accurate census we also must encourage people to respond. As in past decennial censuses, we will mount a robust Communications and Partnership Program to encourage everyone to respond, including those who are traditionally hard to count. People may be hard to count for different reasons, such as those who are highly mobile, homeless, living in remote areas, living in gated communities, or other reasons.

For the 2020 Census, we are building a research foundation for our Integrated Partnership and Communications Program that is stronger than in 2010. We recently conducted the Census Barriers, Attitudes and Motivators Survey (CBAMS), which consisted of two components. First, a quantitative survey was mailed out to 50,000 households. We expect to receive data from this survey in the summer, which will give us important information about the major population

groups in the country. The second component consists of qualitative focus groups that will allow us to hone in on the attitudes and motivators of smaller population groups and populations that cannot be well represented in the quantitative survey, including Native Americans, Alaska Natives, and people who speak languages other than English or are not proficient in English.

The information we receive from CBAMS will be combined with other data at the Census Bureau that we are using to develop models projecting the likelihood of people to respond. Along with the information from CBAMS, this information will provide us with the strongest research foundation we have ever had. These research efforts will help us ensure that our messaging is as effective as possible and that our advertising and partnership efforts are well-directed. Finally, with the support of the recent appropriation, we are looking at other important communications activities and building out our partnership staff earlier than planned.

We recognize that communications and partnerships are at the heart of reaching traditionally hard-to-count populations. Extensive advertising in media consumed by specific populations is critical. In addition to traditional media, we will be active in digital media and on the Web. Our advertising and partnership support materials will be in multiple languages and we will develop and implement a Statistics in Schools program that will help young people understand the importance of responding to the census so that they can take the message home to their families.

We also plan to strengthen our national and local partnerships. We are currently reaching out to major corporations and national organizations, two years ahead of Census Day, so that they can build support for the 2020 Census into their business plans. This is the earliest we have ever started this effort. In addition, seasoned partnership specialists, many with decades of experience, have been working since January 2017 to help tribal, state, and local governments develop Complete Count Committees, which bring leaders and government officials together to develop plans to support the 2020 Census. As we ramp up to 1,000 partnership specialists in FY 2019, our goal is to exceed the 248,000 community partners we had in 2010. Our partners are the trusted voices in communities across the country. They include schools, hospitals, clinics, legal aid centers, faith-based organizations, and businesses large and small. Census partners help people understand that responding to the census is safe and important, and that their responses are confidential and protected by law.

Our efforts to reach traditionally undercounted populations do not stop with communications and partnerships. Through our language program, we will make it possible to respond to the Census in 12 languages, in addition to English, covering nearly 99 percent of the population, or 87 percent of those with limited English proficiency. Language support materials will be provided in a total of 59 languages, and we are developing templates to help our partners carry our messaging in the languages and dialects spoken by small population groups throughout the country.

To reach people who live in different places and situations, the Integrated Partnership and Communications Program will be the most tailored in our history. In fact, most of the operations we have mentioned—from our field operations, to our communication and partnership efforts, to our language program—are designed to reach people who live in different places or situations. We tailor our operations for rural areas and for areas that have experienced natural disasters.

With that in mind, we also would like to share that we recently made the decision to extend the Update Leave operation that we described earlier across the entire Commonwealth of Puerto Rico. This will help us ensure that our address list is correct and that we are adapting to any changes caused by Hurricane Maria. We will make similar changes to other areas as necessary, including the Gulf States impacted by flooding, and those parts of the Western states that experienced wildfires. We also conduct a specific operation in remote Alaska that starts in January of 2020 before the tundra thaws and many people leave their villages. These are only some of the many other examples of the steps we take to adapt our operations to the unique places where people live.

Finally, we are asking federal, state, and local leaders to encourage their constituents to stand up and be counted. We ask that leaders remind the public that the answers they provide on a census form are confidential and protected by law. It is important that community leaders ensure the public knows that census answers may not be used for law enforcement or any other purpose that would reveal a person's identity or how an individual responded to a question. The Census Bureau is bound by Title 13 of the United States Code. This law not only provides authority for the work we do, but also provides strong protection for the information we collect from individuals and businesses.

Anyone who handles census data swears an oath for life to keep those data confidential. Under Title 13, private information is never published. It is against the law to disclose or publish private information. The information the Census Bureau collects cannot be used for any reason except to produce statistics, and violations of Title 13 are punishable by fines and up to five years in prison. The Census Bureau trains every employee, including its field enumerators, on the importance of protecting private information and the importance of the oath, as well as the fact that penalties for violating this law are applicable for a lifetime. Public encouragement and reassurance of this law and our commitment to protecting confidentiality would help achieve our goal of a complete and accurate census in 2020.

2020 Census Activities Supported by the FY 2019 President's Budget

Looking forward, the FY 2019 President's Budget requested \$3.8 billion for the Census Bureau, which includes \$3.1 billion to support the 2020 Census. As noted above, the Census Bureau appreciates Congress' support for the decennial census and the inclusion of an additional \$1.1 billion beyond the program's estimate for 2018 (including contingency funds) in the 2018 Omnibus appropriations act. These funds will help provide financial certainty to the program as we transition from FY 2018 to FY 2019, and represent a down payment on the \$3.1 billion requested in 2019 to continue all preparatory activities and existing field operations.

As we move into 2019, we will undertake a wide range of simultaneous activities designed to finalize preparations for the 2020 Census as outlined in the President's budget. Key activities for the 2020 Census will take place in 2019. We will make final refinements for all systems to ensure they meet all requirements, are secured, are tested, and are seamlessly integrated. The field offices and other field infrastructure must be stood up nationwide in 2019, with the first 40 Area Census Offices (ACO) opening between January and March of 2019, and the remaining 208 offices opening in the summer of 2019. The ACOs will house the managers, staff, materials,

and equipment needed to support the hundreds of thousands of Census Bureau employees conducting local census operations.

Partnership Specialists will work throughout 2019 to build the network of more than 300,000 census partners who will be the trusted voices to encourage communities across the nation to respond to the 2020 Census. In October 2018, we will begin the full-scale development and implementation of all aspects of the communications program, including the establishment of the media spend plans, messaging, and the creative treatments of the advertising campaign. This work lays the foundation for our first advertising buys for the 2020 Census in May 2019.

In 2019, we will conduct the first major field operation for the 2020 Census, which is the In-Field Address Canvassing we mentioned earlier. In this operation, we send field staff to check the accuracy of the addresses in areas that are the most difficult to canvass and cannot be updated by the In-Office Address Canvassing Operation. Approximately 76,000 address canvassing listers and supervisors will be trained and sent into the field to complete this difficult and important work from mid-August to early October of 2019. Recruitment for this operation will take place in the spring of 2019, with training beginning in summer 2019. The operation itself will begin in late summer and stretch to early fall.

The physical printing of the majority of the paper materials for the 2020 Census will begin in June 2019. We also will finalize and secure all of the operations and systems related to the use of administrative records and third-party data and ensure they are working together in preparation for use in the 2020 Census.

Both the 2020 Census and the American Community Survey are essential to the Census Bureau's mission to serve as the leading source of data about our nation's people and economy. All of the censuses and surveys we conduct are important, and we appreciate Congress' support for our work. With less than two years until Census Day, though, we think the Congress is appropriately focused on the 2020 Census, and as you can see, we are now moving ahead at full speed. Much work remains, but we are well-positioned to get it done so that we can conduct a complete and accurate 2020 Census. We look forward to answering your questions.