Exhibit 8

Version Number: 01-2015

U.S. Department of Commerce
Bureau of the Census

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

Reviewed by: [signature] 4/19/18, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

LISA MARTIN

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

For Dr. Catrina D. Purvis

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

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

Unique Project Identifier: 006-000400700

Introduction: System Description

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

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

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

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

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

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

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

(c) any information sharing conducted by the system

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

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

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

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

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

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

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

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

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.
Existing System, No New Security Risks.

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

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

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

Section 2: Information in the System

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

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

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

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

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

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

Other Information (specify)

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

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

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

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

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

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

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

Section 3: System Supported Activities

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

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

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

Section 4: Purpose of the System

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

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Research, Improvement/support of Census Bureau programs through use of administrative and other non-survey data, Quality assurance, and statistical purposes.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, 1) describe how the PII/BII that is collected, maintained, or disseminated will be used. 2) Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

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

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

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

Section 6: Information Sharing and Access

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	
DOC bureaus		X	
Federal agencies		X	
State, local, tribal gov't agencies		X	
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Data is made available to approved researchers on the RDC and CES internal servers, the researchers are Sworn Census employees, Contractors or Special Sworn Status.	X		

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

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

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

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

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

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

Section 7: Notice and Consent

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

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

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

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

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

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

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

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

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: In the case of aggregated secondary data there is no direct contact with the individual.

Section 8: Administrative and Technological Controls

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

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

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. (Similar to 6.2, technical controls and leakage management)

The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following: • Intrusion Detection | Prevention Systems (IDS | IPS) • Firewalls • Mandatory use of HTTP(S) for Census Bureau Public facing websites • Use of trusted internet connection (TIC) • Anti-Virus software to protect host/end user systems • Encryption of databases (Data at rest) • HSPD-12 Compliant PIV cards • Access Controls The Census bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a DLP solution as well.

Section 9: Privacy Act

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

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

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

Section 10: Retention of Information

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

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

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

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

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

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

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

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

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

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

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

Section 12: Analysis

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

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

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

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