U.S. Department of Commerce
Bureau of the Census

Privacy Impact Assessment
for the
CEN14 Longitudinal
Employer-Household Dynamics (LEHD)

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

MICHAEL TOLAND Digitally signed by MICHAEL TOLAND
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=MICHAEL TOLAND, 0.9.2342.19200300.100.1.1=13001000249566
Date: 2018.07.03 12:11:35 -04'00'

for Catrina 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
Longitudinal Employer-Household Dynamics (LEHD)

Unique Project Identifier: 006-00401000

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 Longitudinal Employer-Household Dynamics (LEHD) IT system (CEN14) maintains a secondary collection of administrative records. The Research and Methodology Directorate of the U.S. Census Bureau has a program area known by the same name, i.e., the LEHD program. The LEHD program is a partnership with the 50 states, the District of Columbia, Puerto Rico and the Virgin Islands, in which state-level unemployment insurance, wage record, and establishment (ES-202) administrative records are combined with Census Bureau records. The result creates a longitudinal national frame of jobs and a data infrastructure that describes the dynamics of the U.S. economy and society. The Census Bureau's goal in implementing this LEHD program is to:

1. Improve the quality and relevance of economic and demographic data,
2. Provide better information to decision-makers at the federal, state and local levels,
3. Reduce costs and improve processing efficiencies for the Census Bureau.

The LEHD IT system processes personally identifiable information (PII) such as SSN, name, gender, age, race/ethnicity, date and place of birth, home address, and education. The system also processes business identifiable information (BII) such as work address, salary and work history. Modern statistical and computing techniques are used to combine federal and state administrative data on employers and employees with core Census Bureau censuses and surveys while protecting the confidentiality of people and firms that provide the data.

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

The Quarterly Workforce Indicators (QWI) data product generated by the LEHD program is created via a statistical matching of state partner labor information data and administrative data from other agencies such as the Internal Revenue Service (IRS), Office Personal Management (OPM) and the Census Bureau. State labor data is submitted electronically to the LEHD program where it undergoes a series of data conversions that removes all PII. The QWI is a public use file that provides information on the relationship between employers and employees without exposing any specific information about each.

CEN14 is internally categorized into two distinct subsystems: the Production subsystem and Web subsystem. The Production subsystem is an entry point of data and does the mission-critical processing of data. The LEHD Web subsystem hosts the LEHD-related web

applications. LEHD Web is the only LEHD system exposed to the public. LEHD Web provides the public a way to access public use data.

(c) any information sharing conducted by the system
LEHD receives information from State Partners. The information is passed to CEN13 CES where it is scrubbed of all PII and BII and then returned to CEN14.

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

13 U.S.C. Sections 6 and 9.

(e) the Federal Information Processing Standard (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.
____ 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 that does not 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		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): UI account numbers					
*Explanation for the need to collect, maintain, or disseminate the Social Security Number, including truncated form: Use of SSN maintains longitudinal job histories of all workers, distinguishing one employee from another in order to produce employment dynamics statistics.					

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

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number		g. Salary	X
b. Job Title		e. Email Address		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		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		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		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify): N/A This is a secondary collection, no collection from individuals.					

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

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
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.)* None.

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 that raise privacy risks/concerns. *(Check all that apply.)* None.

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			
X	There are not any IT system supported activities that 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.			

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).

1) The PII/BII is used to create a longitudinal national frame of jobs and a data infrastructure that describes the dynamics of the U.S. economy and society.

2) The PII/BII identified in Section 2.1 of this document 'Information in the System' is in reference to members of the public.

The LEHD IT system maintains a secondary collection of records obtained from state-level unemployment, insurance, wage record and establishment (ES-202) administrative records combined with Census Bureau records. Only pubic use data is disseminated.

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	
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 is not 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 other IT system(s) authorized to process PII and/or BII. Data comes in through the CEN31 ADSD IT system and goes to CEN14 LEHD IT system, The LEHD IT system sends it to the CEN13 IT system where it is scrubbed. Once scrubbed, the data is sent back to the CEN14 LEHD IT system. The LEHD 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/data_protection.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: The LEHD IT system neither collects nor interfaces with the individuals whose PII/BII is collected/maintained. The LEHD maintains a secondary collection of records and has no contact with individuals. This system of records maintained by this IT system is exempt from access and contest requirements as they are statistical records covered under Title 13.

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: The LEHD IT system neither collects nor interfaces with the individuals whose PII/BII is collected/maintained. The LEHD maintains a secondary collection of records and has no contact with individuals. This system of records maintained by this IT system is exempt from access and contest requirements as they are statistical records covered under Title 13.

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: The LEHD IT system neither collects nor interfaces with the individuals whose PII/BII is collected/maintained. The LEHD maintains a secondary collection of records and has no contact with individuals. This system of records maintained by this IT system is exempt from access and contest requirements as they are statistical records covered under Title 13.

Section 8: Administrative and Technological Controls

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

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In 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.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Publications are cleared with the Disclosure Review Board.

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

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 the 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-9, Longitudinal Employer Household Dynamics (LEHD):

	https://www.federalregister.gov/documents/2015/10/30/2015-27719/privacy-act-of-1974-altered-system-of-records
	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: 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 Schedule NC1-29-84-1 Schedule 8
	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	X
Degaussing	X	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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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 indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
X	Quantity of PII	Provide explanation: The collection is for Census Bureau Censuses, therefore, a serious or substantial number of individuals would be affected if there was loss, theft, or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, or the PII itself may result in serious harm to the individual or organization such as name, address, and phone numbers of a list of people who have filed for retirement benefits.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with 13 U.S.C. 9.
X	Access to and Location of PII	Provide explanation: The PII/BII 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-. Backups are stored at Census Bureau-owned facilities.
	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.