

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



**Privacy Threshold Analysis  
for the  
CEN14 Longitudinal  
Employer-Household Dynamics (LEHD)**

**U.S. Department of Commerce Privacy Threshold Analysis**

**Bureau of the Census/ CEN14 Longitudinal  
Employer-Household Dynamics (LEHD)**

**Unique Project Identifier: 006-00401000**

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:** *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

The Longitudinal Employer-Household Dynamics (LEHD) is classified as 'other'. The LEHD IT system processes PII and BII information while protecting the confidentiality of people and firms that provide the data.

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

Data comes in through the CEN13 ADSD IT system and goes to the CEN14 LEHD IT system. The LEHD IT system sends data to the CEN13 IT system where it is scrubbed. Once scrubbed the data is sent back to the CEN14 LEHD IT system.

*c) System location*

The (LEHD) IT system is housed at the Bowie Computing Center (BCC).

*d) The purpose that the system is designed to serve*

The LEHD IT system maintains a secondary collection of administrative records. 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. 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.

*e) The way the system operates to achieve the purpose*

The LEHD program is a partnership with the 50 states, District of Columbia, Puerto Rico and the Virgin Islands, stat-level unemployment insurance, wage record, and establishment administrative records are combined with Census Bureau records. A longitudinal national frame of jobs and a data infrastructure is created that describes the dynamics of the US economy and society.

*f) A general description of the type of information collected, maintained, use, or disseminated by the system*

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 LEHD IT system also processes business identifiable information (BII) such as work address, salary and work history.

*g) Identify individuals who have access to information on the system*

The general public can access public-accessible data. Only Government Employees and Special Sworn Status (SSS) Contractors have access to the system and information on the system.

*h) How information in the system is retrieved by the user*

Publically accessible data is retrieved through LEHD Web.

*i) How information is transmitted to and from the system*

Data comes in through the CEN31 ADSD IT system and goes to the CEN14 LEHD IT system. The LEHD IT system sends it to the CEN13 IT system where it is scrubbed of all PII and BII information. Once it is 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 other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series.



**Questionnaire:****1. What is the status of this information system?**

- \_\_\_\_\_ This is a new information system. *Continue to answer questions and complete certification.*
- \_\_\_\_\_ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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

- \_\_\_\_\_ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- 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 (version 01-2015 or later). *Skip questions and complete certification.*

**2. Is the IT system or its information used to support any activity which may raise privacy concerns?**

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- \_\_\_\_\_ Yes. *Please describe the activities which may raise privacy concerns.*

☐ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?  
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

☐ Companies

☐ Other business entities

☐ No, this IT system does not collect any BII.

#### 4. Personally Identifiable Information

- 4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

☐ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☐ DOC employees

☐ Contractors working on behalf of DOC

☐ Members of the public

\_\_\_\_\_ No, this IT system does not collect any PII.

***If the answer is "yes" to question 4a, please respond to the following questions.***

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

\_\_\_\_\_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

\_\_\_\_\_ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

\_\_\_\_\_ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

\_\_\_\_\_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

***If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.***



### CERTIFICATION

  X   I certify the criteria implied by one or more of the questions above **apply** to the CEN14 LEHD and as a consequence of this applicability, I will perform and document a PIA for this IT system.

       I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Lucia Foster \_\_\_\_\_

Signature SO:  Date: 3/22/18

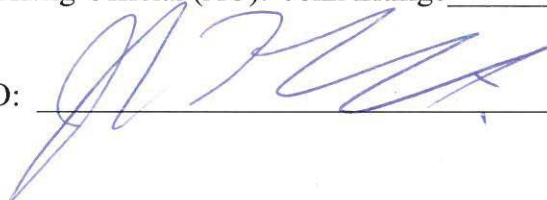
Name of Chief Information Security Officer (CISO): Timothy Ruland \_\_\_\_\_

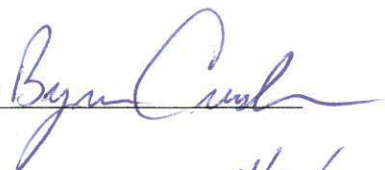
Signature of ITSO/ CIO:  Date: 4/3/2018


Name of Authorizing Official (AO): Kevin Smith \_\_\_\_\_

Signature of AO:  Date: 4/13/18

Name of Authorizing Official (AO): John Eltinge \_\_\_\_\_

Signature of AO:  Date: 3/22/2018

Name of Bureau Chief Privacy Officer (BCPO): Byron Crenshaw 

Signature of BCPO:  Date: 4/17/18