Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Office of the Chief Information Office (OCIO)
Chief Technology Office (CTO)
Enterprise Data Lake (EDL)

Reviewed by: Bryon Crenshaw, 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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2023.03.09 11:18:17 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/Enterprise Data Lake

Unique Project Identifier: FISMA (CSAM) ID 2735

Introduction: System Description

Provide a brief description of the information system.

Office of the Chief Information Officer (OCIO) Chief Technology Office (CTO) Enterprise Data Lake (EDL) is a major application that will provide a Platform-as-a- Service (PaaS) for IT system and data owners, hosting all U.S. Census Bureau surveys data, from collection to tabulation, administrative records, and third-party data. The consolidation of survey processing systems will help the U.S. Census Bureau (USCB) to sustain its place as a leader in statistical methodologies and data products.

EDL is an enterprise-wide, big data management platform that modernizes data storage and data analysis capabilities across all its directorates with appropriate role-based access control. EDL supports the Census Bureau's data and analytical needs in a secure, scalable, high-performing storage and computing cloud environment with appropriate backups to the Census datacenter. This platform increases the Census Bureau's capability to ingest the ever-increasing volume of administrative records, improve the quality of data products and apply disclosure avoidance to protect PII data as required by Title 13, Title 26, and other data protection laws. The EDL will fully support the Process, Derive, and Publish stages of the data lifecycle.

Address the following elements:

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

Enterprise Data Lake is a major application.

(b) System location

The Enterprise Data Lake will reside on the Amazon Web Services (AWS) GovCloud environment. The GovCloud environment is dispersed across two regions: US- East and US-West. AWS headquarters is in Seattle, Washington. AWS and the EDL perform data backups, that are stored at Census Bureau's datacenter located in Bowie, MD.

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

EDL utilizes and interconnects with Cloud Services account for Amazon Web Services (AWS). EDL also interconnects with the IT systems that provide the common enterprise security systems for access and authorization controls such as OCIO Data Communications, OCIO Network Services, OCIO Enterprise Applications, and OCIO Office of Information Security (OIS) Systems. EDL will host data for the Decennial Census, Economic Programs, Demographic Surveys, and the American Community Survey.

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

The IT system was created to support the Census Bureau's longstanding leadership in data analytics and technology. The EDL makes use of AWS Infrastructure-as-a-Service (IaaS), which is a form of cloud computing that provides computing resources over the internet.

EDL provides a PaaS and Software as a Service (SaaS) to its Census Bureau program areas seeking to consolidate data analytics, data management and data storage activities. EDL consolidation of IT systems will allow program areas to leverage standardized data services to centrally govern the programs' data to deliver timely, consistent, and accurate data products.

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

Census Bureau Program data stakeholders will use an interface based on appropriate access and control rights. The user will be able to retrieve the information using a web-based user interface to access or process the data based on his/her role and permissions. Via the web- based user interface, the user can spin up computing environments and load data. The interface will trigger several data processing activities such as batch and interactive processing. This capability provides authorized users visibility into the data transformations that occur, as raw uploaded data moves to the final data product that is published and used for research.

Users with a need to know can retrieve data in EDL by unique identifiers (i.e. JBID, username, and password).

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

EDL receives survey data from the IT systems that are utilized by Census Bureau survey program areas. The program area IT systems will upload survey data from present and past surveys and administrative records data where the Social Security Number (SSN) has been replaced with a unique non-identifying code called a protected identification key (PIK). The data ingested is stored in the storage layer of the EDL and made available for program area consumption after the necessary access approvals are obtained. The EDL will make use of secure tools to ingest data. EDL cloud service providers do not have access to the encryption keys of Census Bureau data therefore they do not have access to the data.

(g) Any information sharing

The EDL system makes data available to Census Bureau program areas that have been authorized to conduct data analytics and management activities involving the information collected from internal census survey systems.

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

13 U.S.C. 8(b), 182, and 196; 3 U.S.C., Chapter 5, 8(b), 131, 132, and 182; 13 U.S.C. 6(c), 141 and 193 and 18 U.S.C. 2510-2521; 13 U.S.C. 196. These collections are conducted under procedures published at 15 CFR, Part 50; 13 U.S.C. 6 and 9; 13 U.S.C. 141 and 193; 13 U.S.C. Chapter 9, Section 301(a), Foreign Trade Statistical Regulations or its successor document, the Foreign Trade Regulations, both in Title 15, CFR part 30; and Title 19, CFR 24.5, and Executive Order 13695, 26 U.S.C. 6103

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

The 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.

____ 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		f. Commercial Sources		i. Alteration in Character	

Management Changes				of Data	
j. Other changes that create new privacy risks (specify): Addition of FTI data					

____ 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.

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

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship		n. Religion	X		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
Geographic information such as Geocodes, GPS coordinates zip codes, county codes, and state codes form part of the survey data record. This information is collected in two ways: the respondents fill/ provide it via the survey instruments/questionnaires and, it is provided by the Geography division within the US Census Bureau via data updates.

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

Enterprise Data Lake (EDL) is an enterprise level platform for survey and/or data program areas to be able to analyze and manage their data they request to be stored in the EDL environment. These program areas are responsible for assuring the data they collect and transmit to EDL is accurate. The accuracy of the data is managed by each program area during their processing and analysis phases which are executed by approved personnel. The EDL will also maintain lineage of data as it is modified so that the original source dataset is preserved.

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		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): The USCB collects, maintains, and disseminates data to support the mission of the agency. See URL for more information https://www.census.gov/about/what.html			

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 USCB collects, maintains, and disseminates data to support the mission of the agency: Survey and third-party data that is ingested and maintained by EDL is provided by the Census Bureau program areas and/or the survey owners from the respective survey areas that are conducting mission-related studies. These surveys include PII and BII from members of the United States public, which may include federal employees and contractors, and personnel of business entities. The data will be used by EDL users to provide data management, processing, analytics, and storage services to Census Bureau program areas.

To promote information sharing initiatives: The Enterprise Data Lake serves as the data storage and processing hub for the Census Bureau, enabling it to support information sharing initiatives. Users will access EDL to process and analyze data from various Census programs and surveys. The data and datasets in EDL will be used to carry out mission related studies and analysis that are disseminated to and within the Census Bureau, other federal agencies, and/or the public.

5.2 Describe any potential threats to privacy, such as insider threat, 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 U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders – both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/FTI Title 13/Title 26 data. In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII/FTI 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 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/FTI 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.

The EDL will also have strict data access controls enforcement capability. In addition, the survey data and administrative records with PII/BII/FTI in EDL will be encrypted both at rest and in motion. In order to offer the maximum-security protection to all U.S. Census Bureau users and stakeholders, the EDL cloud environment is both Federal Risk and Authorization Management Program (FedRAMP) as well as FISMA certified. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Finally, the data stored in the EDL is subjected to encryption when it is stored and when it is used. The EDL has multiple levels of encryption to ensure a greater security. The information in the EDL is handled, retained, and disposed of in accordance with appropriate

federal record schedules. The EDL will also have strict data access controls enforcement capability. The information in EDL is handled, retained, and disposed of in accordance with appropriate federal record schedules.

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			
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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: EDL utilizes and interconnects with Cloud Services account for Amazon Web Services (AWS). EDL also interconnects with the IT systems that provide the common enterprise security systems for access and authorization controls such as OCIO Data Communications, OCIO Network Services, OCIO Enterprise Applications, and OCIO OIS Systems. EDL will host data for the Decennial Census, Economic Programs, Demographic Surveys, and the American Community Survey. EDL 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. Rules of behavior and acceptable use documents must also be signed in addition to Census Bureau mandated awareness training**.**
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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): Researchers under Sworn Status and allowed to access Census environment			

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 This system is a repository of information transferred from other systems. Notice is provided at the point of collection.	
	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: This system is a repository of information transferred from other systems. There is not an opportunity to decline at the EDL system level. The opportunity to decline would occur at the point of collection.

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: This system is a repository of information transferred from other systems. There is not an opportunity to consent to particular use at the EDL system level. The opportunity to consent to particular use occurs at the point of collection.

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: This system is a repository of information transferred from other systems. There is not an opportunity to consent to particular use at the EDL system level.

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/FTI 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, Content of Audit records.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 07/22/2022 ☐ 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.
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. *(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 PII/BII/FTI 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

AWS (Amazon Web Services) provides several security capabilities and services to increase privacy and control network access which includes the following:

EDL will use encryption at rest settings for AWS storage resources. Encryption keys will be stored within a FIPS 140-2 standard validated key store. Where possible, data in transit will be encrypted using Transport Layer Security (TLS) connections to endpoints. Communications that traverse the account boundary of the EDL environment will route through an AWS Virtual Private Network (VPN) Gateway that will provide IPSEC (IP Security) tunnel communications between the EDL environment and external EDL communications. Network Access Controls will be configured to allow only trusted network subnets access to EDL network segments. Security group configurations will further isolate network resources based on IP addresses, Ports, and Protocols. EDL also utilizes data analytics resources to provide end-to-end data security. The analytics use a holistic approach security feature that include:

- Administration
- Authentication and perimeter security
- Authorization
- Audit
- Data protection

Also, EDL is in a dedicated Virtual Private Cloud with continuous monitoring operated by the Census Bureau's Computer Service Division (CSvD).

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X_ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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. *(list all that apply)*: 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, Demographic Survey Collection (Non-Census Bureau Sampling Frame) http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html COMMERCE/CENSUS-8, Statistical Administrative Records System- 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/DEPT-25, Access Control and Identity Management System https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.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: **DAA -0029-2019-0004 : 2020 Decennial Record Schedule** **GRS 5.2 : Transitory and Intermediary 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, and does not have to be 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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Combined data elements uniquely and directly identify individuals.
X	Quantity of PII	Provide explanation: A severe or catastrophic number of individuals affected by loss, theft, or compromise. Breach would cause severe or catastrophic 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 itself may result in severe harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: 13 U.S.C. § 9 requires that data collected by the Census Bureau in its surveys, including the Decennial Censuses, shall remain confidential. Federal tax information will be retained and disposed of in accordance with 26 U.S.C. 6103.
X	Access to and Location of PII	Provide explanation: PII is 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. Backups are stored at contractor-owned facilities and Census Bureau facilities.
	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 two biggest potential threats to privacy regarding EDL are:
1. EDL will be hosted on the out-sourced Amazon Web Services (AWS) GovCloud environment and datacenters which are not managed by Census Bureau employees.
2. Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists.

The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know.

In order to offer the maximum-security protection to all USCB users and stakeholders, the EDL cloud environment is both FEDRAMP as well as FISMA certified. In addition, data stored in the EDL will continue to have the same Title 13 & Title 26 protections. EDL users must take all the USCB mandatory Data Stewardship and Title Data annual training to maintain access to the EDL data. The EDL will also have strict data access controls enforcement capability in addition to detailed audit logs.

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.