Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Associate Director for Research and Methodology (ADRM) Center for Optimization and Data Science (CODS) Cloud Research Environment (CRE)

Reviewed by: Byron 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

BYRON CRENSHAW Digitally signed by BYRON CRENSHAW
Date: 2023.01.24 09:45:10 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
Bureau of the Census, Associate Director for Research and Methodology (ADRM) Center for Optimization and Data Science (CODS) Cloud Research Environment (CRE)

Unique Project Identifier: [Number]

Introduction: System Description

Provide a brief description of the information system.

The Center for Optimization and Data Science (CODS) Cloud Research Environment (CRE) includes data maintained by the Census Bureau's Associate Director for Research and Methodology (ADRM). The CRE system is a cloud-based environment which allows researchers to work with data regarding research projects that support the Census Bureau mission. CRE provides an environment to use and leverage Census data that is stored within a cloud environment. The CRE solution produces a functional cloud environment hosted on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances that are securely configured provide users with a preconfigured solution environment for the analysis of large datasets. The information maintained by CRE is personally identifiable information (PII) and business identifiable information (BII) from the Census Bureau, other government agencies, and data providers. Record linkage using PII/BII facilitates research to improve and support existing Census Bureau programs and the creation of beta data products. These products use innovative techniques that leverage existing data and reduce the burden on respondents. This PII/BII includes members of the public, businesses, contractors, and federal employees. To the maximum extent possible and consistent with the kind, timeliness, quality, and scope of the statistics required under Title 13 of the United States Code, the Census Bureau is required to obtain and use data from other agencies in lieu of direct inquiries through censuses or surveys.

Address the following elements:

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

Cloud Research Environment (CRE) is a general support system

(b) System location
AWS GovCloud Region US West (N. California)

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

CRE interconnects with the Integrated Research Environment (IRE). CRE and IRE are both within the ADRM authorization boundary.

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

The CRE provides a modern research computing environment (infrastructure and software applications as well as economic and demographic data) in the commercial cloud for the Census Bureau Associate Directorate for Research and Methodology (ADRM) researchers. Researchers utilize the data and software applications furnished to their project by CRE to develop and execute research models to analyze and answer specific research questions related to their project.

The information maintained by CRE is personally identifiable information (PII) and business identifiable information (BII) obtained from other Census Bureau program areas. Record linkage, using BII and PII, 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.

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

The data files are stored on disk in various formats determined by the statistical software that they are to be processed with (statistical analysis system (SAS), Stata, R, etc.). Users use these statistical software packages to analyze the data. Data may also be stored in relational databases and retrieved through database queries. Retrieval of the data is performed only by authorized Census Bureau staff who have a need to know and are authorized through Data Management System (DMS).

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

Information is encrypted in accordance with Commerce requirements and sent using a virtual private network (VPN) between CRE and other Census Bureau IT Systems. The VPN offers the required encryption.

(g) Any information sharing conducted by the system

CRE shares PII and BII with other Center for Optimization and Data Science (CODS) components. CRE does not connect or share data external to the Census Bureau.

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

Title 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.

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

Moderate

Section 1: Status of the Information System

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

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

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

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card		m. Medical Record	X
e. File/Case ID	X				
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	X
e. Age	X	l. Email Address	X	s. Physical Characteristics	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship	X	n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
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		f. 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):					

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.

The verification and validation of the accuracy of the data in the CRE is part of the data ingest and storage process. That process is outside of the CRE. The data used for research computing has therefore already been validated for accuracy before it is used inside the CRE. While in use within the CRE, the data is accessible only to users that are authorized to use the data for their research computing project.

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

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

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	
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): The system is being used for demographic and economic research and statistical purposes.			

Section 5: Use of the Information

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

Research, improvement/support of Census Bureau programs through use of administrative and other non-survey data, quality assurance, and statistical purposes:
Record linkage using PII/BII 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.

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/Title 13/Title 26 data.

In addition, 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 an email Data Loss Prevention solution.

The information in the CRE is handled, retained, and disposed of in accordance with appropriate 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		
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: CRE connects with and receives PII/BII data from the ADRM CODS IRE system. The CRE 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 email 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.

6.4 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): 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.

	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.

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.

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 comprised of data that is transferred from other internal systems.

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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): __June 30, 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 5 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 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 DOC 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).*

All data resides in Amazon Web Services (AWS) GovCloud (environment is specific only for Federal customers), and data is protected by disk level encryption and database encryption. AWS GovCloud has an existing ATO (Authority to Operate) under FedRAMP, which gives Government agencies the ability to leverage AWS GovCloud for sensitive workloads. The following are specific to AWS:

1) Cloud enclave is an extension of the Census Network
2) All data/processes are in AWS GovCloud, FedRAMP approved
3) All systems are in a virtual private cloud (VPC) with controls and security groups
4) All data is encrypted at rest and in motion

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 an enterprise email DLP solution as well.

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-2, Employee Productivity Measurement Records- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-2.html COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html COMMERCE/CENSUS-4, Economic Survey Collection- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/CENSUS-7, 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/CENSUS-12, Foreign Trade Statistics- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-12.html

	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1 General Technology Management Records, GRS 3.2 Information Systems Security Records; GRS 4.3 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	
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 serious or substantial number of individuals affected by loss, theft, or compromise. Serious 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, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: The context of use for CRE system is for demographic and economic research and statistical purposes.
X	Obligation to Protect Confidentiality	Provide explanation: Data is protected by Title 13 Section 9.
X	Access to and Location of PII	Provide explanation: The PII is physically located on servers owned and managed by a AWS Gov Cloud at offsite facilities located in the United States. AWS Gov Cloud is a Federal Risk and Authorization Management Program (FedRAMP)-approved Cloud Service Provider (CSP).
	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.)

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.

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.

Points of Contact and Signatures

System Owner
Name: Robert Sienkiewicz
Office: Center for Optimization and Data Science
Phone: 301.763.1234
Email: robert.sienkiewicz@census.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: ROBERT SIENKIEWICZ Digitally signed by ROBERT SIENKIEWICZ Date: 2022.12.05 15:35:51 -05'00'
Date signed:

Chief Information Security Officer
Name: Beau Houser
Office: Office of Information Security
Phone: 301.763.1235
Email: beau.houser@census.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2023.01.05 12:56:06 -05'00'
Date signed:

Privacy Act Officer
Name: Byron Crenshaw
Office: Policy Coordination Office
Phone: 301.763.7997
Email: Byron.crenshaw@census.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.01.24 09:45:38 -05'00'
Date signed:

Agency Authorizing Official
Name: Luis Cano
Office: Office of the Chief Information Officer
Phone: 301.763.3968
Email: luis.j.cano@census.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2023.01.05 14:48:01 -05'00'
Date signed:

Bureau Chief Privacy Officer
Name: Byron Crenshaw
Office: Policy Coordination Office
Phone: 301.763.7997
Email: Byron.crenshaw@census.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.01.24 09:45:59 -05'00'
Date signed:

Business Authorizing Official
Name: John Eltinge
Office: Office of the Associate Director for Research & Methodology
Phone: 301.763.9604
Email: john.l.eltinge@census.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: JOHN ELTINGE Digitally signed by JOHN ELTINGE Date: 2023.01.10 11:47:38 -05'00'
Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.