Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Office of the Chief Information Officer (OCIO) Enterprise Applications

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: 2022.09.20 16:08:31 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/Office of the Chief Information Officer (OCIO)
Enterprise Applications

Unique Project Identifier: 006-000401400

Introduction: System Description

Provide a brief description of the information system.

The response must be written in plain language and be as comprehensive as necessary to describe the system

The OCIO Enterprise Applications system is the functional management framework used to deliver applications to end users of the U.S. Census Bureau network. OCIO Enterprise Applications contains a variety of systems and applications that maintain or collect personally identifiable information (PII). They are:

- enterprise-level data tracking systems;
- general support systems for internal data management,
- transaction-based systems, and
- relational database management systems

Address the following elements:

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

The OCIO Enterprise Applications system is comprised of both a variety of systems and applications.

(b) System location

OCIO Enterprise Applications resides at the following locations:

- Bowie, Maryland
- AWS GovCloud is located in Oregon and Ohio

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

OCIO Enterprise Applications systems interconnects with infrastructure services at the U.S. Census Bureau. This includes OCIO Data Communications for authentication/ telecommunication purposes, OCIO Network Services for server/storage, and OCIO Client Support Division (CSD) for laptops and workstations.

In addition, the OCIO Enterprise Applications systems interconnect with the following Census Bureau:

- Office of the Chief Information Officer (OCIO) Administrative Systems Vol II
- Associate Director for Demographic Programs (ADDCP) Decennial
- Office of the Chief Information Officer (OCIO) Field
- Associate Director for Demographic Programs (ADDP) Demographic Census, Surveys, and Special Processing
- Office of the Chief Information Officer (OCIO) Centurion
- Office of the Chief Information Officer (OCIO) Human Resources Applications
- Associate Director for Field Operations (ADFO) National Processing Center
- Associate Director for Research and Methodology Systems (ADRM) Cloud Research Environment
- Office of the Chief Administrative Officer (OCAO) Lenel
- Associate Director for Economic Programs (ADEP) Economic Census and Surveys and Special Processing
- Office of the Chief Information Officer (OCIO) Commerce Business Systems
- Office of the Chief Information Officer (OCIO) Cloud Services
- Office of the Chief Information Officer Enterprise Tools and Development Services (ETDS)
- Office of the Chief Financial Officer (OCFO) Budget Systems
- Office of the Chief Information Officer (OCIO) Office of Information Security (OIS) Systems
- Associate Director for Economic Programs (ADEP) Foreign Trade Division Applications
- Other OCIO Enterprise Applications systems.

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

The purpose of the enterprise-level data tracking systems is to ensure data consistency, data integrity, and generate meaningful data information through data management, tracking, and reporting for Census Bureau collections. Another capability is an enterprise-wide analytics platform for surveys and censuses. This system allows statisticians within census and survey projects to perform statistical models using census and survey response data, paradata, administrative records, and many other types of data. The system will receive PII including Identifying Numbers, General Personal Data, and Work-Related Data. The PII is received from other information systems that collect, maintain and disseminate Census and Survey data.

The general support systems for OCIO Enterprise Applications provide internal data management within the Census Bureau collections. This system allows users to request access to datasets, and when approved, users are granted access to the datasets within a secure environment provisioned by the system. Census Bureau datasets are for internal use by employees and are capable of containing protected or administrative information.

The transaction-based systems within OCIO Enterprise Applications serve as the primary mechanism for operational control across surveys for data collection. The system can be considered an operational brain that determines operational workflow based on pre-existing protocols.

The relational database management systems store and retrieve data as requested by other software applications. This system provides both a testing, development and production environment for optimum functionality.

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

For the enterprise-level data tracking system, authorized users can use their roles and privileges to retrieve information by personal identifiers. For the enterprise-wide analytics platform for surveys and censuses, information can be retrieved by personal identifiers, however this is not a normal function of the enterprise-wide analytics system.

For the general support systems for internal data management, information can be retrieved by personal identifiers.

For the transaction-based systems, authorized users can use their roles and privileges to retrieve information by personal identifiers.

For the relational database management system, authorized users can use their database roles and privileges to retrieve information by personal identifiers.

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

Information is transmitted securely via Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS).

(g) Any information sharing

The enterprise-level data tracking system does not share information. The enterprise-level analytics system is an environment for use by researchers to make decisions during the data collection phase of a survey or a Census. The system will provide the researcher with any data that they request as input and will output and send decision-based data only to other systems.

This could include things such as case level intervention codes, a stop work decision, or best time of day to contact respondents. The system does not provide a mechanism for sharing PII/BII with other systems.

The general support system shares information within the Census Bureau by querying indexed metadata and by sending email to data owners, administrators, and other application users.

The relational database management system does not share information.

The transaction-based system shares demographic survey, Decennial, and Economic Census information within the Census Bureau and with the Department of Commerce, that is used to determine new survey content, support electronic collections, for statistical purposes, and to create datasets for the Census Bureau.

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

5 U.S.C. 301
13 U.S.C. Chapter 9, and Sections: 6, 8(b), 9, 131, 132, 141, 161, 182, 193, 196
15 C.F.R. Part 30 and 19 C.F.R. Section 24.53
18 U.S.C. 2510-2521
26 U.S.C. 6103(j) and
Foreign Trade Statistical Regulations or its successor document, the Foreign Trade Regulations

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

The FIPS 199 security impact category for Enterprise Applications 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.
_____ 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		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card	X	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	
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	
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)

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	X	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 OCIO Enterprise Applications is part of the data ingest and storage process. The data used within OCIO Enterprise Applications has already been validated for accuracy before it is pulled inside the OCIO Enterprise Applications. While in use within OCIO Enterprise Applications, the data is accessible only to users that are authorized to use the data. The initial Authorization To Operate (ATO) and the Information Systems Continuous Monitoring program provides an ongoing monitoring of data accuracy as maintained by security controls derived from NIST 53A. System and Communications (SC) provides Protection of Policy and Procedures, Application Partitioning, Information in Shared Resources, Denial of Service, Information System Boundary, Transmission Confidentiality & Integrity, and Cryptographic Protection. In addition, System and Information Integrity (SI) provides Flaw Remediation Protection, Malicious Code Protection, Inbound and Outbound Communications Traffic monitoring protection, System-Generated Alerts, etc.

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	X	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): For 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).

The PII/BII maintained for administrative purposes: This IT system maintains first name, last name, address, email address, etc. to ensure that mandatory survey or statistical, information is ready for internal Census use. The information pertains and is in reference to federal employees/contractors conducting the surveys and the public.

The PII/BII maintained for statistical and research purposes: The data maintained by this IT system is collected from other IT systems that collect censuses and surveys (e.g., responses and statuses) and is used to direct data collection efforts. It is also used to inform program areas within the Census Bureau (responsible for survey and census questionnaire mail out) whom to send survey and census forms to. The IT system gathers response data from the data collection modes to send it to the survey and census processing IT systems in a standardized way. This information enables the Census Bureau to fulfill its legal obligation to provide mandated statistics. The information pertains to members of the public.

The PII/BII maintained for information sharing initiatives: This information is collected and shared within the Census Bureau and the Department of Commerce to create datasets for various types of censuses and surveys. This information enables the Census Bureau to fulfill its legal obligation to enhance its information sharing initiatives. The information pertains to members of 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. 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 information in OCIO Enterprise Applications 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	X
DOC bureaus	X		
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?

X[1]	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.
	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.

[1] External Agencies/Entities are required to verify with the Census Bureau any re-dissemination of PII/BII to ensure consistency with the Memorandum of Understanding (MOU)/inter-agency agreement and the appropriate SORN.

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: • OCIO Administrative Systems • ADDCP Decennial • OCIO Field and ECase • ADDP Demographic Census, Surveys, and Special Processing • OCIO Centurion • OCIO Human Resources Applications • ADFO National Processing Center • ADRM Cloud Research Environment • OCAO Lenel • ADEP Economic Census and Surveys and Special Processing • OCIO Commerce Business Systems • OCIO Cloud Services • OCIO Enterprise Tools and Development Services (ETDS) • OCFO Budget Systems • OCIO Office of Information Security (OIS) Systems • ADEP Foreign Trade Division Applications 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 facilities that house Information Technology systems.
	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):			

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: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to decline to provide PII/BII at the OCIO Enterprise Applications system level.

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: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to consent to particular uses of PII/BII at the OCIO Enterprise Applications system level.

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: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to review/update PII/BII at the OCIO Enterprise Applications 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 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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): ____ July 20, 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 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.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	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).*

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 Census 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

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 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.

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 CENSUS-4, Economic Survey Collection: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5, Decennial Census Programs: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/CENSUS-7, Special Censuses of Population Conducted for State and Local Government: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html COMMERCE/CENSUS-8, Statistical Administration Records Systems: 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 4.1 - Records Management Records GRS 4.2 - Information Access and Protection Records GRS 4.3 - Superseded by July 2017 by GRS 5.1 and GRS 5.2 (GRS 5.1 - Common Office Records & GRS 5.2 - Transitory and Intermediary Records) **Demographic Directorate** N1-29-99-5: National Prisoner Statistics Program Capital Punishment (NPS-8) Reports N1-29-89-3: Surveys Collected Under Title 15 of the U.S. Code N1-29-87-3: Survey of Fishing, Hunting and Wildlife Associated Recreation, 1980 and Later - Electronic Records (Inactive) N1-29-86-3: Current Population Survey (CPS) - Electronic Records (Inactive) NC1-29-85-1: Survey of Income and Program Participation (SIPP), 1979 and Thereafter NC1-29-79-7: Demographic Fields Area (DFA) Records Schedule **Economics Directorate** N1-029-10-2: Business Register System N1-029-10-3: Standard Economic Processing System (StEPS) N1-029-12-004: Economic Directorate Document Management System (EDMS) N1-029-10-4: Micro Analytical Database (MADb) Company Statistics Division N1-29-10-1: Survey of Business Owners & Self - Employed Persons Program Records **Economic Surveys Division** N1-29-03-1: Economic Surveys NC1-29-80-15: Surveys of Manufacturers, 1960, Sample Detail File, Backup File and Survey of Persons with College Degrees on II-A and III-A Tape (Inactive) NC1-29-79-4: Economic Census and Organization Survey Data Files , 1972 - 74 (Inactive) NC1-29-78-15: Economic Surveys Division Data Files on II-A Tape (Inactive) NC1-29-78-8: Extracts from Commodity Transportation Surveys, 1963 - 72 (Inactive) **Manufacturing and Construction Division** NC1-29-81-10: Records Schedule - Construction Statistics Division **Decennial Directorate** N1-29-05-01: Respondent Data from the 2004 Overseas Enumeration Test N1-29-10-5: 2010 Census Records Schedule **American Community Survey** DAA-0029-2015-0001: American Community Survey Records for 2007 and Thereafter
	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	
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: PII/BII collected can be directly used to identify individuals
X	Quantity of PII	Provide explanation: The collection is for demographic, Economic Surveys, and other surveys, and therefore, a severe or catastrophic number of individuals would be affected if there was loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII/BII, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the act of collecting and using the PII/BII in this IT system or the PII/BII itself may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance Title 13 collections. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: PII/BII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access is limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals. Access is only allowed by organization-owned equipment outside of the physical locations, and only with a secured connection.
	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: Gregg D Bailey
Office: Office of the Chief Information Officer
Phone: 301-763-0989
Email: gregg.d.bailey@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: GREGG BAILEY
Digitally signed by GREGG BAILEY
Date: 2022.08.25 09:53:43 -04'00'

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: 2022.09.13 14:36:01 -04'00'

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: 2022.09.20 16:09:03 -04'00'

Date signed:

Authorizing Official
Name: Luis J. 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: 2022.09.15 13:19:03 -04'00'

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: 2022.09.20 16:09:24 -04'00'

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.