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

## Privacy Impact Assessment
## for the
## Center for Optimization and Data Science (CODS)
## Integrated Research Environment (IRE)

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: 2023.01.10 10:42:38 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date
(Or the BCPO if this is an existing system that is eligible for an annual certification)

# U.S. Department of Commerce Privacy Impact Assessment
# Bureau of the Census, Center for Optimization and Data Science (CODS)
# Integrated Research Environment (IRE)

**Unique Project Identifier: 006-000400700**

## <u>Introduction</u>: System Description

*Provide a brief description of the information system.*

The Center for Optimization and Data Science (CODS) Integrated Research Environment (IRE) includes data maintained by the Census Bureau's Associate Director for Research and Methodology (ADRM). The IRE system is an on-premises environment which allows researchers to work with data regarding research projects that support the Census Bureau mission. IRE covers the personally identifiable information (PII) and Business identifiable information (BII) from each of the research centers maintained by the system. The ADRM data holdings include census and survey data including PII and BII received from other Census Bureau IT systems identified in item c below, administrative records from other federal, state, and local agencies, and proprietary data files from commercial vendors and some non-profit organizations. 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. By reusing data that already exists elsewhere, and linking it to census and survey data, Census is able to conduct research that provides a more holistic view of the people present in, and the economy of, the United States. Information received from administrative records are protected from unauthorized disclosure under Title 13 U.S.C. 6. The data in IRE is used for statistical purposes and for research and operations to improve record linkage methods for surveys, including the decennial census.

Address the following elements:

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

The Center for Optimization and Data Science IRE is a general support system

*(b) System location*

Bowie, Maryland

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

The Center for Optimization and Data Science IRE interconnects with the following Census systems:

IRE interconnects with the following Census Bureau systems:

- ADEP ITO: Associate Directorate for Economic Programs
- ADEP EAD: Economic Census and Surveys and Special Processing
- ADDCP GEO: Geography
- ADDP DSD: Demographic Census, Surveys and Special Processing
- OCIO CAES: Concurrent Analysis and Estimation System
- DIR DMS: Data Management System
- ADDCP ACSO: American Community Survey
- ADEP ITMD: Foreign Trade Division Applications
- ADDCP DSCMO-DSSD: Decennial
- ADEP UTS: Unified Tracking System
- ADEP IDMS: Identification Management System
- ADEP ERD: Economic Reimbursable Surveys Division

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

CODS IRE provides a research platform with high performance computing and standard statistical tools to conduct research for improvement/support of Census Bureau Programs through use of administrative and other non-survey data, quality assurance, research, improvement/support of Census Bureau Programs and statistical purposes. The research platform interacts with the Census Data Management System (DMS), the Identification Management System (IDMS) and the Center for Enterprise Dissemination (CED) Management System (CMS) to make sure the research projects are approved and creates project space for the project on the research platform. The system provides access to project space only for the users that have been approved to work on the project. The project has access only to the data that it has received prior approval to track functions for research proposal and active projects. The DMS is used to track the status and activity of all projects from initial conception through completion and close out.

For external Federal Statistical Research Data Center (FSRDC) users, the CED CMS is used to perform management and tracking functions for research proposals and active projects. The CMS is used to track the status and activity of all projects from initial conception through completion and close out. Data is available only to researchers who have received prior approval.

*(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 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 DMS.

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

Data is transmitted by Secure File Transfer Protocol (SFTP) and Linux based tool to synchronize files between systems.

*(g) Any information sharing*

The Center for Optimization and Data Science does not share data with any external IT systems.

The Center for Optimization and Data Science uses the DMS to share data with the following internal systems:

IRE uses DMS to share data with the following:

- ADEP ITO: Associate Directorate for Economic Programs
- ADEP EAD: Economic Census and Surveys and Special Processing
- ADDCP GEO: Geography
- ADDP DSD: Demographic Census, Surveys and Special Processing
- OCIO CAES: Concurrent Analysis and Estimation System
- ADDCP ACSO: American Community Survey
- ADEP ITMD: Foreign Trade Division Applications
- ADDCP DSCMO-DSSD: Decennial
- ADEP ERD: Economic Reimbursable Surveys Division

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

13 U.S.C. §§ 6 and 9.

*(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 | |
| 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. Marital Status | 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 | | k. Procurement/contracting records | |
| d. Work Telephone Number | X | h. Employment Performance Ratings or other Performance Information | X | | |
| 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 | | e. ID Files Accessed | |
| 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 | X | Other Federal Agencies | X |
| State, Local, Tribal | X | Foreign | | | |
| Other (specify): | | | | | |

| **Non-government Sources** | | | | | |
|---|---|---|---|---|---|
| Public Organizations | | Private Sector | X | Commercial Data Brokers | X |

| | | | |
|---|---|---|---|
| Third Party Website or Application | | | |
| Other (specify): Some data is received from non-profit organizations | | | |

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 CODS IRE is part of the data ingest, curation and storage process. The data used for research computing has already been validated for accuracy before it is used inside this system. While in use within the Center for Optimization and Data Science IRE, 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?

| | |
|---|---|
| X | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection.<br>OMB 0607-0995 Generic Clearance for Collection of State Administrative Records Data |
| | 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): Research, Improvement/support of Census Bureau Programs through use of administrative records and other non-survey data, quality assurance, 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 Center for Optimization and Data Science IRE data will be used in the following ways:<br><br>Research improvement/support of Census Bureau programs through use of administrative records and other non-survey data, quality assurance, and statistical purposes:<br>Record linkage using BII and Protected Identification Keys (PIKs) 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 can 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 National Institute of Standards and Technology (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 hypertext transfer protocol secure (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 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 (DLP) solution.

The information in IRE is handled, retained, and disposed of in accordance with appropriate federal record schedules.

## <u>Section 6</u>: 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): Access to data is made available to approved researchers on the FSRDC and CODS internal servers, the researchers are Sworn Census employees, Contractors or Special Sworn Status. | X | | |

| | |
|---|---|
| | 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.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:<br>CODS IRE interconnects with the following Census Bureau organizations for sharing/receiving:<br>Connects with the following to share data with:<br>• ADEP ITO: Associate Directorate for Economic Programs<br>• ADEP EAD: Economic Census and Surveys and Special Processing<br>• ADDCP GEO: Geography<br>• ADDP DSD: Demographic Census, Surveys and Special Processing<br>• OCIO CAES: Concurrent Analysis and Estimation System<br>• DIR DMS: Data Management System<br>Connects with the following to receive data from:<br>• ADDCP ACSO: American Community Survey<br>• ADEP ITMD: Foreign Trade Division Applications<br>• ADDCP DSCMO-DSSD: Decennial |

| | |
|---|---|
| | - ADEP UTS: Unified Tracking System<br>- ADEP IDMS: Identification Management System<br>- ADEP ERD: Economic Reimbursable Surveys Division<br><br>This system uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including 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 in transit and at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise 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: IRE is a repository of information transferred from other systems. The opportunity to decline, if existing, would be in the originating IT system/agency. |

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: IRE is a repository of information transferred from other systems. The opportunity to consent, if existing, would be in the originating IT system/agency. |

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: IRE is a repository of information transferred from other systems. The opportunity to review/update PII/BII, if existing, would be in the originating IT system/agency. |

## 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.<br>Explanation:<br>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-5. 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.<br>Provide date of most recent Assessment and Authorization (A&A): 06/30/2022<br>☐ 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).*

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 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 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 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).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br>COMMERCE/CENSUS-2, Employee Productivity Measurement Records- |

| | |
|---|---|
| | http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-2.html<br>COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies<br>http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html<br>COMMERCE/CENSUS-4, Economic Survey Collection-<br>http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html<br>COMMERCE/CENSUS-5, Decennial Census Program-<br>http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html<br>COMMERCE/CENSUS-7, Demographic Survey Collection (Non-Census Bureau Sampling Frame)-<br>http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html<br>COMMERCE/CENSUS-8, Statistical Administrative Records System-<br>http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-8.html<br>COMMERCE/CENSUS-9, Longitudinal Employer Household Dynamics System-<br>http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-9.html<br>COMMERCE/CENSUS-12, Foreign Trade Statistics-<br>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.<br>Provide the name of the record control schedule:<br>GRS 3.1 General Technology Management Records,<br>GRS 3.2 Information Systems Security Records;<br>GRS 5.1 Common Office Records<br>DAA-0029-2014-0005: Records of the Center for Administrative Records Research and Applications. |
| | No, there is not an approved record control schedule.<br>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 | 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:<br>Individual data elements directly identifying unique individuals. |
| X | Quantity of PII | Provide explanation:<br>A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic 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:<br>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:<br>Disclosure of the act of collecting, and using the PII, or the PII itself is likely to result in severe or catastrophic harm to the individual or organization. |
| X | Obligation to Protect Confidentiality | Provide explanation:<br>Organization or Mission- specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government- wide or industry-specific requirements. Violations may result in severe civil or criminal penalties. |
| X | Access to and Location of PII | Provide explanation:<br>Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization’s workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization- owned equipment outside of the physical locations owned by the organization 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.<br>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.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required technology changes. |