Template Version Number: 01-2021

U.S. Department of Commerce
Census Bureau

Privacy Impact Assessment
for the
Associate Director for Economic Programs (ADEP)
Innovation and Technology Office (ITO)

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL Date: 2024.04.18 15:42:03 -04'00' 1/18/2024

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau ADEP ITO Applications

Unique Project Identifier: 006-00402100 00-07-01-02-01-00

Introduction: System Description

Provide a brief description of the information system.

The ADEP ITO system is comprised of major applications that:

- Provide users the ability to design how paper, internet, computer assisted, and/or telephone assisted instruments should appear (e.g., what questions should be asked, when they should be asked, etc.), and provide users the ability to design how their respondent materials should appear (e.g., define the contents).
- Perform paper-based data collection activities that facilitates the Batching, Scanning, Registration, Interpretation, Quality Control Measurement, Error Containment, as well as an Exception Review process while providing scanned digital images of respondent questionnaires in real time.
- Provide Census Bureau analysts secure access to the 2010 and 2020 census data and the digital images of the questionnaires from which the data were captured to support comprehensive and accurate reviews, evaluations, and research.
- Provide survey operational control functionality needed to support field, internet, and telephone data collection operations.
- Provide a cloud-based data exchange Application Programming Interface (API), in partnership with a cloud vendor, that allows business entities - e.g., commercial and public (local and state government) – to electronically transfer economic survey data to the Census Bureau. This exchange will allow Census to receive information from a broader set of entities more rapidly, thereby providing Census access to better, more timely economic indicators and information on the U.S. economy.

Address the following elements:

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

ADEP ITO system is a general support system that is comprised of major applications.

(b) System location

ADEP ITO system is hosted within the following locations:

- National Processing Center (NPC) in Jeffersonville, Indiana
- Census Bureau's Bowie Computer Center (BCC) in Bowie, Maryland
- Amazon Web Services (AWS) GovCloud (US-East) Region located in the Northeastern United States

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

ADEP ITO interconnects with systems within the Associate Director for Economic Programs (ADEP), Associate Director for Field Operations (ADFO), Associate Director for Decennial Census Programs (ADDCP), and Office of the Chief Information Officer (OCIO).

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

ADEP ITO system is designed to:

• Provide users the ability to design how paper, internet, computer assisted, and/or telephone assisted instruments should appear (e.g., what questions should be asked, when they should be asked, etc.), and provide users the ability to design how their respondent materials should appear (e.g., define the contents).

• Perform paper-based data collection activities that facilitates the Batching, Scanning, Registration, Interpretation, Quality Control Measurement, Error Containment, as well as an Exception Review process while providing scanned digital images of respondent questionnaires in real time.

• Provide Census Bureau analysts secure access to the 2010 and 2020 census data and the digital images of the questionnaires from which the data were captured to support comprehensive and accurate reviews, evaluations, and research.

• Provide survey operational control functionality needed to support field, internet, and telephone data collection operations. Operational control functionality includes manages cases, regardless of mode and case type, by creating operational workloads, pushing these cases to the data collection instruments, and tracking key status and events for each case during the data collection lifecycle. Information is also received from a OCIO Human Resources system and collected about Census Bureau employees during the collection of respondent information. Field representative and interviewer characteristics obtained during census and survey interviews, pilot tests, and cognitive interviews are used for research and analytical studies to evaluate Census Bureau surveys and programs.

. • Provide batching of survey responses. Business entities who elect to participate, will do an extract of their financial information that they would normally be asked to provide to Census by responding to numerous surveys. The vendor software will then perform some basic validations and formatting, and then would send that data to the OCIO Census Bureau enterprise respondent system, via the API. This exchange will allow Census to receive information from a broader set of entities more rapidly, thereby providing Census access to better, more timely economic indicators and information on the U.S. economy.

ADEP ITO system operates by:

Design instruments: Provides a user interface where staff have the ability to design how their paper, internet, computer assisted, and/or telephone assisted instruments should appear, provides valid users the ability to design how their respondent materials should appear, and provides central repository for all metadata required for the generation of instruments and respondent materials.

Paper-based data collection operations: Creates scanned digital images of respondent questionnaires, detects presence of and captures checkmark responses, detects presence of and captures write-in responses, allows clerical keying for write-in responses not captured, reprocesses sampled paper data to provide error correction and containment, provides detailed tracking of each step in the paper processing workflow and provides reports on processing status, progress, and issues/exceptions.

Secure Access: Provides Census Bureau analysts secure access to the 2010 and 2020 census data and the digital images of the questionnaires from which the data were captured.

Survey Operational Control: Provides staff with a user interface to support field, internet, and telephone data collection operations throughout the data collection lifecycle.

Batching of Survey Responses: Software as a Service that provides batching of survey responses coming from company source systems into singular JSON files in preparation for delivery to the OCIO Census Bureau enterprise respondent system. Functionality includes survey data structure and integrity validation prior to submission to the OCIO Census Bureau enterprise respondent system.

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

Information within the ADEP ITO system is retrieved by authorized users using internal web interfaces, application programming interfaces, secure databases, and managed file transfer servers. Information contained within the system is not available to the public. Only authorized

Census Bureau federal employees and contractors with a need-to-know have access to the system. Data is searchable/retrievable by PII.

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

Information is transmitted to and from the system by using secure point-to-point connections, application program interfaces (API), database replications, and secure Manage File Transfer methods. Secure communications are employed with layered security controls including, but not limited to the use of validated FIPS 140-2 cryptographic modules and mechanisms to protect PII/BII.

(g) Any information sharing conducted by the system

ADEP ITO system interconnects and shares information with systems within the Associate Director for Economic Programs (ADEP), Associate Director for Field Operations (ADFO), Associate Director for Decennial Census Programs (ADDCP), and Office of the Chief Information Officer (OCIO).

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

15 U.S.C. 301.
13 U.S.C. Chapter 5, 6(c), 8(b), 131, 132, 141, 161, 182, 193, 196
26 U.S.C 6103

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

The FIPS 199 rating for ADEP ITO system is Moderate.

Section 1: Status of the Information System

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

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	

c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Addition of Software as a Service (SaaS)					

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

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
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		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		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	h. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	i. Employment Performance Ratings or other Performance Information			

j. 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 Scan	
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
k. Other system administration/audit data (specify):					

Other Information (specify)
Federal Tax Information such as: Business name, legal form of business, business revenue, number of employees, Business 1040 data, Title 26 Administrative Data, and North American Industry Classification System (NAICS).

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	X	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	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

ADEP ITO system use a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (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, data validation controls to ensure accuracy of information. It is the responsibility of the internal sponsor to vet system information for accuracy and transform it into a format that the external sponsor can ingest.

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 no ADEP ITO 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	
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): Collected for statistical purposes, to shape and guide public policy, and to aid in identifying federal funding needs			

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).

Census Bureau information shapes important policy and operational decisions that help improve the Nation's social and economic conditions. We conduct the constitutionally mandated Census of Population and Housing every ten years, which is used to apportion seats in the House of Representatives and informs congressional redistricting. The PII collected, maintained, and/or disseminated by ADEP ITO major applications is in reference to members of the public.

We also conduct a census of all business establishments and of all governmental units, known respectively as the Economic Census and the Census of Governments, every five years. The Economic Census is the benchmark used for measuring Gross Domestic Product (GDP) and other key indicators that guide public policy and business decisions.

In addition, we conduct several ongoing business and household surveys that provide the information in several of the Nation's key economic indicators, which are used to allocate over $400 billion in Federal funding annually.

The PII/BII collected for statistical purposes: The PII/BII maintained is from voluntary and mandatory surveys, census interviews, pilot tests and cognitive interviews collected from member of the public.

The PII collected for administrative purposes: ADEP ITO collects information about Census Bureau employees during the collection of respondent information. Field representative and interviewer characteristics obtained during census and survey interviews, pilot tests, and cognitive interviews are used for research and analytical studies to evaluate Census Bureau surveys and programs.

5.2 Describe any potential threats to privacy 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 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 Data Loss Prevention (DLP) solution.

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			
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: ADEP ITO system connects to systems within the Associate Director for Economic Programs (ADEP), Associate Director for Field Operations (ADFO), Associate Director for Decennial Census Programs (ADDCP), and Office of the Chief Information Officer (OCIO). ADEP ITO uses security controls mandated by (FISMA and various other regulatory control frameworks including NIST special publications. These security controls include but are not limited to the use of mandatory Hypertext Transfer Protocol Secure (HTTPS) for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption for data at rest, and various physical controls at the Census Bureau facilities that house information technology systems. The Census Bureau also deploys an enterprise DLP solution.
	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	
X	Yes, notice is provided by other means.	Specify how: Privacy Act statements are provided at the point of collection. Individuals are informed by one of the following: Privacy Act Statement upon login, letter, interview, or during data collection.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII.
X	No, individuals do not have an opportunity to decline to provide	Specify why not: For mandatory surveys or censuses, the respondent does not have an opportunity to decline.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII for some questions.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Some Census Bureau surveys are mandatory as required by 13 U.S.C. Individuals are informed of this by one of the following: Privacy Act Statement upon login, letter, interview, or during data collection.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: If the Census Bureau contacts the respondent for an update then the respondent can provide the updated information. For some Census Bureau surveys, individuals have the opportunity to provide updates to PII data within the submitted survey or survey website.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For surveys covered under System of Record Notices (SORNs) Census-4 and Census-5 there are no access & contest requirements since the data is collected for statistical purposes.

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 systems are audited and monitored per U.S. Census Bureau Enterprise Audit procedures.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ____06/30/2023_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Publications are approved by the Disclosure Review Board

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.

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). 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 Programs: 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/DEPT-25, Access Control and Identity Management System: https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html SORNS that cover data received from OCIO Human Resources system: COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-1.html OPM/GOVT-5, Recruiting, Examining, and Placement Records: https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-3-records-of-adverse-actions-performance-based-reductions-in-grade-and-removal-actions-and-terminations-of-probationers.pdf OPM/GOVT-7, Applicant Race, Sex, National Origin, and Disability Status Records: https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-7-applicant-race-sex-national-origin-and-disability-status-records.pdf
	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: N1-29-98-1 N1-029-05-2 N1-029-10-3 NC1-29-82-4 N1-029-10-4 NC1-29-82-4, Item 56 N1-29-92-1, Item D or 12c DAA-0029-2013-0004
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same 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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Data elements are not directly identifiable

		alone but may indirectly identify individuals
X	Quantity of PII	Provide explanation: Although a serious or substantial number of individuals would be affected by loss, theft, or compromise, the PII collected and maintained is non-sensitive which is unlikely to result in harm to individuals.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, have little relevance outside the context.
X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, or the PII itself is unlikely to result in harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.
X	Access to and Location of PII	Provide explanation: The PII/BII is located on computers (including laptops) and networks, and IT systems controlled by the Census Bureau. Access is limited to those with a need to know including the Census Bureau geographic program area, regional offices, and survey program offices, etc.
	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.