Version Number: 01-2021

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

Privacy Impact Assessment
for the
Associate Director for Field Operations (ADFO) National Processing Center (NPC)

Reviewed by: Donna Neal (Acting), 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

Tahira Murphy for Charles Cutshall 8/29/23

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/ Associate Director for Field Operations (ADFO)
National Processing Center (NPC)

Unique Project Identifier: 006-00403600

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 survey information collected in ADFO NPC components are wide ranging and contain Business Identifiable (BII) Information and Personally Identifiable Information (PII). Some of the economic survey information collected are employer identification number, addresses, financial, and transactional data. An example of some of the demographic and economic surveys processed by ADFO NPC components are: The American Community Survey, Company Organization Survey, Special Censuses, and the Survey of Income and Program Participation. ADFO NPC also houses and manages call center collection. Data is captured for aggregation. Calls to respondents are recorded for coaching, quality control, and falsification investigations. Recordings reside in an encrypted format on dedicated servers and are used by authorized monitors, coaches, or managers. Access is granted through an application using Remedy ticket control system. Collection online is for business, demographic, and agricultural data.

Address the following elements:

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

The Associate Director for Field Operations (ADFO) National Processing Center IT (NPC) system is a General Support system.

(b) System location

The ADFO NPC is located at the Census Bureau's National Processing Center (NPC) in Jeffersonville, IN with Paper Data Capture Centers (PDCCs) in Jeffersonville, IN and Phoenix, AZ and Call Centers (CCs) at Jeffersonville, IN and Tucson, AZ.

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

The ADFO NPC is connected to the same Wide Area Network as the Census Bureau in Suitland and Bowie, Md. Internal connections are documented with Interconnection Security Agreements (ISA). Other inputs and outputs to the United States Postal Service for administrative address corrections are guided under publicly available agreements. Partnership agreements with the United States Department of Agriculture provide for data transfer for the Agricultural Census. A Memorandum of Understanding and ISA between the Department of Labor (DOL), Wage and Hourly Division and NPC allows for movement of data from NPC to DOL.

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

A professional Human Resource cadre works with the organizational management to recruit and hire and train a cadre of professional and clerical personnel to staff processes and functions that make up the ADFO NPC systems. Initially, the ADFO NPC receives seed data in the form of addresses from sponsor divisions. The seed data are candidate respondent's addresses. The organization is capable of processing the seed data immediately through telephone interviewers using Computer Assisted Telephone Interviewing (CATI from the Jeffersonville or Tucson Call Centers. NPC also offers Document Services that assist in design and printing forms for mailing consistent with specifications of the sponsoring Divisions. NPC prints addresses on designed instruments then mails them through the United States Postal Service (USPS) with Postal paid return envelopes. The instrument may be a set of instructions or a questionnaire that contains instructions that provide access to sponsor designed and sponsor-maintained WEB interfaces. The respondent decides and either fills the questionnaire and mails it back or follows alternate instructions. Respondent may choose to enter their responses via the Internet (WEB). NPC maintains staff who also have access to the WEB to assist respondents who choose to use that method. NPC processes respondent questionnaires received via USPS using state of the art data capture systems. Raw data is placed on a secure data bus and sent back to the sponsor for aggregation and analysis.

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

Data at the NPC is not available to the public. ADFO NPC might be considered the Census input device for all kinds of data, similar to the keyboard on a computer. Federal workforce and select contractors use dedicated United States Government Computing Base compliant workstations built to rigid Census desktop standards to interface with applicable servers. Secure protocols provide the channel for information to be retrieved by the employees. Users are granted access to data on a need-to-know basis and must use unique credentials over PIV-II standard identification and authentication mechanisms. The data is searchable by unique identifiers.

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

ADFO NPC employs the Census Bureau Enterprise Service Bus (ESB) for data transmissions from dedicated file servers or directories. Secure File Transfer Protocol is used to move the data.

(g) Any information sharing

The ADFO NPC is connected on the same Wide Area Network as the Census Bureau in Suitland and Bowie, Md. Internal connections are documented with Interconnection Security Agreements (ISA) and govern describe the security of the data exchange. Interface Control Documents (ICD) defines the specifications about the data constructs and form. Other inputs and output from the United States Postal Service for administrative address corrections are guided under publicly available agreements. Partnership agreements with the United States Department of Agriculture provide for data transfer for the Agricultural Census. A Memorandum of Understanding and ISA between the Department of Labor (DOL), Wage and Hourly Division and NPC allows for movement of data from NPC to DOL. ADFO NPC receives information from OCIO Commerce Business Systems, ADDCP American Community Survey Office, ADDCP Decennial, ADEP Integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), MOJO Enhanced Operational Control System, and the National Agriculture Statistical Service, and the Department of Labor. Once the information is received, ADFO NPC components process the data and provides access to the finished product to the data sponsor (internally or externally).

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

The system contains data that is confidential in nature, protected by Title 5, Title 13, Title 15 and Title 26 of the US Code, and protected under the Privacy Act.

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

In conformance with the methodology prescribed by FIPS Publication 199, the data sensitivity classification for the US Census Bureau ADFO NPC GSS confidentiality, integrity, and availability 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*	X	f. Driver's License	X	j. Financial Account	
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		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: NPC is a delegated hire authority and maintains personnel and performance information related to employees. NPC performs multiple cross checks with National Finance files based on SSN.					

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	
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship	X	n. Religion	X		
u. Other general personal data (specify):					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording	X	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		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	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
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		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

Keyed data is re-keyed by a dedicated Statistical Methods and Quality Assurance Branch (SMQAB) staff. If a second keyer input is equivalent to the initial keyed data, then the keyed data is considered accurate. If a second keyer provides a different answer, an adjudicator reviews the difference and resolves the inconsistency. Sponsors determine the level of quality assurance based on the capability of the SMQAB professionals.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. Multiple, e.g.: Census of Agriculture OMB 0535-0226; ARM survey OMB 535-2018; Demographics OMB 1850-0598, and many others
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

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

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	X
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	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

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).

For administrative matters: PII is collected from employees and is used for awards, disciplinary actions, eligibility, and promotions.

To improve federal services online: PII/BII is collected from members of the public for demographic surveys, the American Community Survey, and Decennial and Economic censuses. This information is maintained by this IT system to produce statistical information. As the nation's statistical agency, the Census Bureau with assistance from its processing center, NPC, is tasked with data collection, analysis, and publication of the nation's data for statistical purposes.

For administering human resources programs: To track and provide for training, health insurance, leave, performance, and payroll for employees. Fingerprints are collected for applicants for background checks and are delivered via a GSA system to the FBI. They are not retained in GSA systems.

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.

Measures are implemented to ensure data protection for all measures of confidentiality, integrity, and availability. Encryption is implemented for data at rest and in flight to protect the confidentiality of the data. The weakness is execution of process. A rigorous response for any suspected breaches of protocol are immediate and thorough. The BOC CIRT is notified within an hour of suspected breach and trained investigators take remedial action to ensure mitigation. Mandatory training on data stewardship emphasizes the importance of confidentiality and employee response. Integrity is ensured through the use of database systems, hash and check digits for files and units. Availability is ensured through clustering, mirroring, backups and facility and physical environmental controls that are technically state of the art.

The information in the ADFO NPC 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		X	
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.

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: ADFO NPC receives information from OCIO Commerce Business Systems, ADDCP American Community Survey Office, ADDCP Decennial, ADEP Integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), MOJO Enhanced Operational Control System, the National Agriculture Statistical Service, and the Department of Labor. Once the information is received, ADFO NPC components process the data and provide access to the finished product to the data sponsor (internally or externally). Some examples of sharing within the Census Bureau are OCIO Commerce Business Systems, ADDCP American Community Survey Office, ADDCP Decennial, ADEP Integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), MOJO Enhanced Operational Control System, and the National Agriculture Statistical Service. Some external organizations that ADFO NPC has processed survey information for are: The National Agriculture Statistical Service and the Department of Labor. ADFO NPC uses 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 the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.

[1] External agencies/entities are required to verify with the Census Bureau any re-dissemination of PII/BII to ensure consistency with the MOU/inter-agency agreement and the appropriate SORN

	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: via Privacy Act Statements provided to respondents prior to providing responses to a census or survey.
	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: Various surveys ingested by the ADFO NPC IT system are voluntary and therefore individuals are not required to provide PII/BII.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Some surveys and censuses 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.

7.3 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: Various surveys maintained by the ADFO NPC IT system are voluntary and therefore individuals have the opportunity to consent to particular uses of their PII/BII.

X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Some surveys and census data maintained by the ADFO NPC IT system are mandatory as required by 13 U.S.C. The data are used for statistical and administrative purposes only and are exempt from consent to particular uses of PII/BII.

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: For some surveys and census information maintained by the ADFO NPC IT system, individuals have the opportunity to provide updates to PII/BII data on the submitted survey or on the survey website.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For surveys that collect information for statistical purposes, respondents are exempt from review/update of PII/BII unless the Census Bureau contacts them to update the information.

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 within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to IT system processes that handle PII, all manual extractions for PII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _____07/01/2023_____ ☐ 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 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).*

The 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 the Census Bureau's 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
- Full disk encryption
- Encryption in flight
- 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. Associate Director for Field Operations (ADFO) National Processing Center GSS contains, transmits, or processes BII/PII has a current authority to operate (ATO). The system goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well.

Section 9: Privacy Act

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

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

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

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/CENSUS-2, Employee Productivity Measurement Records- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-2.html COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html COMMERCE/CENSUS-4, Economic Survey Collection- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/CENSUS-7, Demographic Survey Collection (Non-Census Bureau Sampling Frame)- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons- https://www.osec.doc.gov/opog/privacyact/sorns/dept-1.html COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies- https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html COMMERCE/DEPT-25, Access Control and Identity Management System- https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html OPM/GOVT-10, Employee Medical File Systems Records- https://www.osec.doc.gov/opog/PrivacyAct/sorns/GOV-Wide/OPM-GOVT-3-opm-sorn-govt-3-records-of-adverse-actions-performance-based-reductions-in-grade-and-removal-actions-and-terminations-of-probationers.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: GRS 2.7 item 10, 60 and 70, GRS 1.1 item 010, GRS 4.2, GRS 5.2 and as specified by the sponsor.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify): Quantities of disks are sent to NSA shredding facility to destroy the hard drive in industrial shredders.			

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 Census Bureau Censuses and surveys, 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 with 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: 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.)

As new people and configurations of systems come on board to process the 2020 Census, the threat from new employee error or intent is a potential threat. The necessity of scaling up to meet the rigors and demands in a tight economic environment with a reduced pool of potential employees makes staffing a particular challenge. Continued training and risk of legal enforcement mitigate for the threat.

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.