Exhibit 6

Version Number: 01-2017

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

Privacy Impact Assessment
for the
CEN08 Decennial Information Technology Division (DITD)

Reviewed by: ______________________, 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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.09.28 19:04:38 -04'00'

09/27/2018

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/CEN08 DITD

Unique Project Identifier: 006-000400400

<u>Introduction</u>: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system. Please answer each question (a) through (i)separately.

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

CEN08 Decennial Information Technology Division (DITD) consists of both general support systems and major applications:

<u>Major Applications</u>

CEN08 Decennial manages the development and implementation of major decennial census applications utilized by the Decennial Census Program. These applications process response data from census tests and 2020 Census operations, and perform quality assurance mechanisms for various census operations. These applications also facilitate the acquisition of software and integration services required to support the U.S. Census Bureau (USCB) during the preparation and actual Decennial Census operations.

Some examples of the information collected, maintained, and/or disseminated within CEN08 Decennial are names, addresses, gender, age, date of birth, race, email, education, telephone number and salary.

The CEN08 Decennial IT system monitors the cost, schedule, and technical performance milestones for each software system or application utilized for decennial census purposes. The CEN08 IT system manages the development and implementation of software and systems necessary to support collection, processing, and tabulation of census data.

<u>General Support System</u>

CEN08 DITD general support system consists of:

1) an external vendor general support system called the Third Party Fingerprinting solution that is managed by Indrasoft. The U.S. Census Bureau (USCB) employs hundreds of thousands of temporary workers to perform data collection activities via a non-competitive Schedule A hiring authority from the Office of Personnel Management (OPM) in support of the Decennial Census testing in Fiscal Year (FY) 2018 and 2020 Census. As part of the recruitment and security process, the USCB requires that these selectees undergo fingerprinting to determine their suitability for employment. In addition, contractors that provide services in support of the 2020 Decennial Census, such as Census Questionnaire Assistance (CQA) contractor candidates, may also be

fingerprinted. To support fingerprinting for the 2020 Census, the USCB will use the Third Party Fingerprinting solution to capture and transmit fingerprints to USCB and conduct identity proofing for these temporary hires and contractors.

2) CEN08 DITD also consists of another external vendor general support IT system called the Recruiting and Assessment (R&A) solution that is managed by Cornerstone OnDemand. R&A is a FedRAMP-approved IT system that allows the Census Bureau to have a recruiting & selection tool and a learning management tool in one. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

(b) System location

Decennial Applications – Bowie Computer Center (BCC) and AWS GovCloud located in Oregon.

Third Party Fingerprinting – AWS U.S. East/West located in US East (Ohio), US East (N. Virginia), US West (N. California), and US West (Oregon) and physical fingerprinting capture sites across the United States.

R&A - Unified Talent Management Suite (CUTMS) Cloud located in El Segundo, CA and Ashburn, VA.

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

Decennial Applications – Shares information internally within the Census Bureau with CEN07 GEO, CEN05 Field, CEN11 DEMO, CEN18 CDL, CEN19 CEDSCI, CEN21 DAPPS, CEN30 ACS, and CEN36 ADEP.

Third Party Fingerprinting – Shares information internally within the Census Bureau with CEN21 CHEC and CEN18 SOA.

R&A – Shares information internally within the Census Bureau with *CEN21 DAPPS*

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

The CEN08 DITD provides updates and unit (e.g., a home, a building, or miscellaneous structure) status information to various divisions within the Census Bureau that maintain address information (e.g., street addresses, and status and control information for households and other living quarters). In addition, CEN08 systems confirm receipt of response data. They also provide validation and acknowledgment of the data received from various IT systems.

Temporary hires and contractors looking to support the 2020 Census submit their job applications through the R&A system. R&A securely delivers the submitted application data and associated attachments to DAPPS for processing and selecting.

To support fingerprinting for the 2020 Census, the USCB will use the Third Party Fingerprinting solution to capture and transmit fingerprints to USCB and conduct identity proofing for temporary hires and contractors (selectees). These selectees will provide their fingerprints at one of the Third Party Fingerprinting physical capture sites.

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

Information in the CEN08 DITD systems are retrieved by using PII information identified in Section 2 below by authorized users using internal web applications, secure databases, and managed file transfer servers. Authorized Census Hiring Employment Check (CHEC) users pull selectee fingerprint files from the Third Party Fingerprinting solution and forward to the FBI for processing.

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

Information is transferred to and from CEN08 DITD systems via authorized manual and/or automated connections.

User fingerprints are captured on Third Party Fingerprinting physical sites which is uploaded to authorized AWS U.S. East/West. Files are encrypted and transferred using the service-oriented architecture (SOA) via the Enterprise Service Bus (ESB), which then sends it over to CHEC within the U.S Census Bureau. The Enterprise Service Bus is a configuration-based, policy-driven enterprise service bus. It provides highly scalable and reliable service-oriented integration, service management, and traditional message brokering across heterogeneous IT environments. It combines intelligent message brokering with routing and transformation of messages, along with service monitoring and administration in a unified software product.

(g) Any information sharing conducted by the system

CEN08 DITD systems share information internally with approved Census Bureau systems on an as needed basis.

Fingerprints are shared between the fingerprinting solution, CHEC and FBI.

R&A Applicant information is shared internally with the Decennial Applicant, Personnel and Payroll System (DAPPS).

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

Title 13, U.S.C. Section 6c
Title 13, U.S.C. Section 141
Title 13, U.S.C. Section 193
44 U.S.C. Section 3101
41 U.S.C. 433(d)
5 U.S.C. 301
5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397
Executive Order 12107
Executive Order 12564

(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.
__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): New Third Party Fingerprinting solution.					

____ 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.

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID	x	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender	x	j. Telephone Number	x	p. Military Service	
e. Age	x	k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity	x	l. Education	x	r. Mother's Maiden Name	
s. Other general personal data (specify): Citizenship					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number		g. Salary	x
b. Job Title		e. Email Address		h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	x	d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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	d. Queries Run	x	f. Contents of Files	
g. Other system administration/audit data (specify): Audit Logs					

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		Other Federal Agencies	x
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	x	Commercial Data Brokers	x
Third Party Website or Application			x		
Other (specify):					

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

CEN08 DITD uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to data validation controls to ensure accuracy of information.

Selectee information is verified for accuracy when individuals schedule their fingerprints by verification against other forms of identification. Further, background checks are performed by the FBI to validate name, credit, and criminal history.

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	x
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	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	x
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	x
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For Statistical Purposes (i.e. Censuses/Surveys)			

Section 5: Use of the Information

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

The PII collected, maintained, and/or disseminated by the CEN08 IT system is in reference to members of the public. Data collection is used to produce national statistical information.

Third Party Fingerprinting is capturing selectee fingerprint data on behalf of the U.S Census Bureauto hire selectees to help conduct the 2020 Census operations. The third party vendor is mandated to only utilize FedRAMP authorized solutions. The vendor does not directly submit the fingerprint information to the FBI, rather the information is securely sent to the U.S Census Bureau for processing and submission to the FBI.

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.)

CEN08 DITD systems adhere to the Information Technology Security Program Policy as it relates to handling, retaining, and disposing collected information. Census Bureau information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes 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 a Data Loss Prevention (DLP) solution as well.

Fingerprints are retained for 120 days and then disposed of following NIST sanitation guidance. All individuals that handle PII are required to complete annual Data Stewardship Awareness training.

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	
DOC bureaus			
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 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: Decennial Applications – Shares information internally within the Census Bureau with CEN07 GEO, CEN05 Field, CEN11 DEMO, CEN18 CDL, CEN19 CEDSCI, CEN21 DAPPS, CEN30 ACS, and CEN36 ADEP. Third Party Fingerprinting – Shares information internally within the Census Bureau with CEN21 CHEC and CEN18 SOA. R&A – Shares information internally within the Census Bureau with CEN21 DAPPS CEN08 uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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: http://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.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Employment with the U.S. Census Bureau is voluntary.
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: According to Title 13, Section 221 (Census, Refusal or neglect to answer questions; false answers) of the United States Code, persons who fail or refuse to respond to the mail-back census form, or refuse to respond to a follow-up Census Bureau taker can be fined up to $100. Persons who knowingly provide false information to the Census Bureau can be fined up to $500. For Census Bureau employees who access systems in CEN08 providing PII is a requirement for employment.

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: Employment with the U.S. Census Bureau is voluntary. Temporary hires and contractors have to consent to the U.S. Census Bureau uses of their PII.
x	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For records covered by SORN Census-5, Decennial Census Programs, there are no access and consent requirements since the data is collected for statistical purposes only. For Census Bureau employees consent to particular uses of PII is a requirement for employment.

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: Selectee information is verified for accuracy when individuals schedule their fingerprints.
x	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For records covered by SORN Census-5, Decennial Census Programs, there is no opportunity to review/update data unless the Census Bureau contacts the respondent for an update on their information. For Census Employees, employees have access to PII via the appropriate Human Resources applications that reside outside of the CEN08 IT system.

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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___July 25, 2018________ [ ] 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.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Census Bureau information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes 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 a Data Loss Prevention solution as well.

Section 9: Privacy Act

9.1 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-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/DEPT-13, Investigative & Security Records- http://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-13.html COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html OPM SORN GOVT-5, Recruiting, Examining and Placement Records- https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-5-recruiting-examining-and-placement-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: Nl-29-05-01, N1-29-10-5, GRS 3.1, GRS 5.6 item 181
	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):			

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.
	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 levels. *(Check all that apply.)*

X	Identifiability	PII collected can be directly and indirectly used to identify individuals.
X	Quantity of PII	The collection is for the decennial census, therefore, a severe or substantial number of individuals would be affected if there was loss, theft or compromise of the data. This could affect decennial 2020 Census response rates and have a long term effect on the Nation's population count. Severe collective harm to the USCB's

		reputation, or cost to the USCB in addressing a breach.
X	Data Field Sensitivity	The PII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
X	Context of Use	Disclosure of PII in this IT system or the PII itself may result in severe harm to the individual or organization.
X	Obligation to Protect Confidentiality	PII collected is required to be protected in accordance with 5, U.S.C (552a) and 13, U.S.C, section 9.
X	Access to and Location of PII	The PII is located on computers (including laptops) and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know including the Census Bureau regional offices and survey program offices, etc. Access is allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities. PII is also located on U.S. Census Bureau authorized vendor systems. Access is limited to those with a need-to-know for authorized U.S. Census Bureau contractors and employees.
	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.)

A third party vendor is capturing selectee fingerprint data and PII on behalf of the U.S Census Bureau. The third party vendor is mandated to only utilize authorized systems and FedRAMP solutions. The vendor does not directly submit the fingerprint information to the FBI, rather the information is securely sent to the U.S Census Bureau for processing and submission to the FBI.

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.