Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Associate Director for Research and Methodology Systems (ADRM)
Focus Groups

Reviewed by: Donna Neal, 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: 2025.05.20 13:35:39 -04'00' 5/20/25

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 Research and Methodology Systems (ADRM) Focus Groups

Unique Project Identifier: [Number]

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 Census Bureau's Center for Survey Methodology uses contractor support for a variety of qualitative pretesting and evaluation research methods, including cognitive testing, focus groups, behavior coding, debriefings, and usability testing to test new questions, materials or technologies, and methods as well as to understand public perceptions of the work of the Census Bureau. The primary purpose of these research projects is to evaluate and improve the effectiveness and efficiency of Census Bureau data collection activities. These projects are relatively small, and varied in nature, and require the ability to quickly parse out this work through multiple subcontractors that offer us different skillsets, facilities, and other resources.

This Privacy Impact Assessment (PIA) covers cognitive interviews and focus groups captured and/or maintained by a third-party contractor. Focus groups and qualitative interviews collect general information on opinions, attitudes and understanding of production Census Bureau data collection instruments. These data are used to evaluate and improve Census Bureau surveys and censuses. This information will be stored on contractor systems. The information collected and maintained will be used by Census Bureau researchers to evaluate and improve the quality of data collection procedures and activities associated with Census Bureau surveys and censuses. Participants may be Census Bureau employees as volunteers or external audiences. Some of the focus groups, debriefings, and/or testing activities may be audio/video recorded or video screen captured by the Census Bureau to help in further evaluation of Census Bureau activities.

The Census Bureau will also use an eye tracking technology to help evaluate the attentiveness and focus of research participants when reviewing Census questionnaires. The eye tracking technology uses a light source to illuminate the eye causing highly visible reflections. An image of the eye is captured by a camera and is used to identify the reflection of the light source on the cornea (glint) and in the pupil. Census research will use this information to calculate a vector formed by the angle between the cornea and pupil reflections. This

information is then used to calculate the gaze direction. The eye tracking technology, including eye images captured by the Census Bureau are done on secure government computers and handled in a manner consistent with federal data protection requirements as detailed in this PIA.

The Federal Government Standards offer a framework for security controls to be implemented for information systems to help achieve more secure information systems and effective risk management within the federal government, including a contractor's information systems. Security controls are the management, operational, and technical safeguards or countermeasures employed within a contractor's information system to protect the confidentiality, integrity, and availability of the system and its information.
The Census Bureau's Office of Information Security (OIS) will review the contractor's documentation to determine the information system's suitability to safeguard information at the moderate-impact system level. The OIS will determine if a contractor's information system meet the IT requirements using the following Federal Government Standards:

- Federal Information Processing Standards (FIPS) 199 – Standards for Security
- FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
- National Institute of Standards and Technology (NIST SP 800-53, Revision 5 – Moderate Impact)
- National Institute of Standards and Technology (NIST SP 800-61, Revision 2), The Federal Incident Reporting Guidelines
- FIPS 140-2 – Security Requirements for Cryptographic Modules

Address the following elements:

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

The IT systems used for ADRM Focus Groups and cognitive testing are typically general support IT systems.

(b) System location

Various contractors will be used on an as needed basis. Contractors who have met the required Federal Government Standard for the protection of information collected, stored, or disseminated on an IT system will be used. In most situations, IT systems used for these types of research projects will be located with the contracted third party at offsite facilities located in the United States. The third-party vendors used are Federal Risk and Authorization Management Program

(FedRAMP) approved Cloud Service Providers (CSPs). Upon completion of each research project, all Census Bureau data is transferred to the Census Bureau for storage. No Census Bureau information will remain with the third party.

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

In most situations, IT systems used are standalone systems. There may be few occasions when focus group and/or cognitive testing activities will use only a secure Census Bureau IT system that interconnects with other secure Census Bureau IT systems.

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

The information collected from ADRM Focus Groups will be used by Census Bureau researchers to evaluate and improve the quality of data collection procedures and activities associated with Census Bureau surveys and censuses. Information collected may also be used to better understand public perceptions of Census Bureau work.

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

Census staff will retrieve the information by aggregate dataset groups, not by personal identifiers, for example interview number assigned to a set, focus group number assigned to a set, etc.

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

The method used for transmitting data will vary depending on the type of study. In most studies transmission of data will be done according to standard for cryptographic-based security systems in Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules. In other studies the transmission of data will be done using Transport Layer Security (TLS), secure file share, or secure file transfer applications such as Secure Shell File Transport Protocol (SFTP) in accordance with Department of Commerce policy regarding the electronic transmission of information, 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, trusted internet connection (TIC) access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Census Bureau IT systems.

The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well to prevent electronic transmission of personally identifiable information without proper encryption.

Once cleared and approved, contractors will provide the information to the Census Bureau through virtual desktop infrastructure (VDI). The Census Bureau provides access to the contractor by way of the Census Bureau's VDI in order to transfer research materials and information to the contractor and for the contractor to transfer collected research results back to the Census Bureau. The contractor will access VDI using contractor computer equipment to share, collaborate, or transmit data. VDI allows a user to access to software applications that are integrated into the Census Bureau's system so not every application is available. Most applications needed for work are available via VDI. Upon clearing the Security Background Investigation, the contracting office representative (COR) will submit a request for a token and schedule VDI training for the contractor. The VDI training is available in-person or via webinar and will not exceed 3 hours.

(g) Any information sharing

Aggregate information will be shared with appropriate Census Bureau staff. Personally identifiable information (PII) collected by the contracted third party will only be shared with other Census Bureau research staff employees.

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

Title 13 U.S.C., Chapter 5, Sections 6(c), 8(b), 131, 132, 141, 182, 193 and 196
5 U.S.C. 301
44 U.S.C. 3101

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

Moderate

Section 1: Status of the Information System

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

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

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

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
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: The PII and/or BII collected as part of the ADRM Focus Groups include questionnaires, notes, recruiting worksheets, consent forms and any other work products created by the contractor.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X[1]
b. Maiden Name		i. Place of Birth	X	p. Medical Information	X[2]
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):					

[1] Does not include financial account information, but only income and program participation.
[2] Only asking for self-assessment of mental health conditions in national emergencies and access to medical or mental health care.

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
c. Work Address[3]	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): Economic Data[4]					

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	X	h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	X	i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Eye tracking technology which include video recording and screen captures a photograph of the exterior of the subjects' eyes[5].					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources

[3] Work Address are business addresses for businesses in Census Economic surveys.
[4] Financial data from businesses, e.g., total annual/quarterly payroll, total receipts/revenue, expenses.
[5] Eye tracking technology does not scan the iris or retina of the eye. It captures a photograph of the exterior of the eye. A description of how this technology is used can be found in the Introduction section of this PIA.

Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

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

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

Focus group and cognitive testing participants are voluntarily recruited. Information provided to the Census Bureau from participants are self-response. For these research studies, incorrect or vague responses provide valuable information to our researchers regarding potential issues with the wording or structure of Census questionnaires. No action(s) are taken or determinations made about specific individuals, including determinations about rights, benefits, or privileges, because of this information.

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. 0607-0725; 0607-0978; 0607-0971
	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): Video recording (non-surveillance) and video screen captures[6]			

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

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
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).

[6] Video screen capture is used in the instance of online data collection. This would simulate video recording the in-person session.

PII will be collected from members of the public and/or federal employees that may be involved in a focus group study to improve Federal Services online and to measure and improve employee and customer satisfaction.

The information collected from focus groups will be used by Census Bureau researchers to evaluate and improve the quality of data collection procedures and activities associated with Census Bureau surveys and censuses. Information collected may also be used to better understand public perceptions of Census Bureau work.

PII will also be collected from Census Bureau employees, contractors, and other federal government personnel, for training surveys and other human resource purposes.

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.

To process federal information, security controls for the Federal Information Security Management Act (FISMA) moderate level is implemented and validated through the FISMA Assessment and Authorization (A&A) process, using the Cyber Security Assessment & Management (CSAM) ATO method. This process includes implementing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, IT security and privacy controls at the moderate level with additional controls and control steps from Census Bureau policies as determined by the RMPS process. These controls include, but are not limited to, account management, authentication, physical controls, and personnel security.

In most studies transmission of data will be done according to standard for cryptographic-based security systems in Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules. In other studies the transmission of data will be done using Transport Layer Security (TLS), secure file share, or secure file transfer applications such as Secure Shell File Transport Protocol (SFTP) in accordance with Department of Commerce policy

regarding the electronic transmission of information, the Federal Information Security Modernization Act of 201 (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, trusted internet connection (TIC) access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Census Bureau IT systems. Upon completion of each research project, all Census Bureau data is transferred to the Census Bureau for storage and purged from the third-party's IT system. No Census Bureau information will remain with the third party.

In addition, all contractors must complete the Census Bureau's Data Stewardship Awareness training covering privacy and IT security procedures prior to handling Census Bureau data.

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	
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: A contracted third-party IT system will be used. Each IT system will be assessed by the Census Bureau's Office of Information Security (OIS) to ensure federal IT requirements using the following Federal Government Standards are met: • Federal Information Processing Standards (FIPS) 199 – Standards for Security • FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems • National Institute of Standards and Technology (NIST SP 800-53, Revision 5 – Moderate Impact) • National Institute of Standards and Technology (NIST SP 800-61r2), The Federal Incident Reporting Guidelines • FIPS 140-2 – Security Requirements for Cryptographic Modules
	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.)*

	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: Research topics will vary. As each research topic is developed a Privacy Notice specific to the research will be written and provided to all participants.
	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: Participation is voluntary. Individuals may refuse to participate in the research or, if they do participate, they may refuse to answer specific questions.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Participants can decide which PII to provide to the Census Bureau. In addition, the privacy notice will provide informed consent specific to each data collection explaining the use of PII. Participants can decline to provide PII.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: ADRM Focus Groups systems are measuring the quality and effectiveness of questionnaires and data collection, therefore we want to capture measurements of question effectiveness instead of the accuracy of responses. Due to this, incorrect or outdated information provided by research participants is valuable to the research as it helps identify areas of potential issues or confusion within certain Census questionnaires of field procedures. Therefore, respondents are unable to review/update their PII. No action(s) are taken on or determinations made about specific individuals, including determinations about rights, benefits, or privileges, because of the information.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	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: The Privacy Compliance Branch maintains an inventory of PII/BII collected, maintained, or disseminated within each IT system that is operated by or on behalf of the Census Bureau.
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): _X__ Accreditation is done at the point of contract award. _June 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.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	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.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII 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 IT systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII will have 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. The DLP is an email scan of unencrypted email messages and attachments to detect inappropriate

transport of sensitive information. In addition, all contracted third party IT systems are required to meet Federal IT security standards identified in the FISMA, including but not limited to the Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, to work on Census Bureau operations. These standards are assessed by the Census Office of Information Security and described in the Request for Proposal (RFP) and detailed within each awarded contract.

Section 9: Privacy Act

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

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

__X__ 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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
X	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: General Record Schedule 3.1 - General Technology Management Records GRS 3.2 - Information Systems Security Records

	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: CSM is nearing completion of our record control schedule.
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify):			

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
X	Quantity of PII	Provide explanation: The sample size for these focus groups and studies are generally small (less than 100 per session). A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: The combination of certain PII items may be sensitive. Sensitive items, if compromised, may result harms, such as identity theft, embarrassment, loss of trust, or costs to study participants and/or the agency.
X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, *or* the PII itself may result in serious harm to the individual or organization

X	Obligation to Protect Confidentiality	Provide explanation: Information collected is protected from unauthorized disclosure by Title 13, U.S.C. Violations may result in serious civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: The PII is physically located on servers owned and managed by a third-party vendor at offsite facilities located in the United States. The third-party vendors used are Federal Risk and Authorization Management Program (FedRAMP) approved Cloud Service Providers (CSPs). PII is also held at the Census Bureau and accessed by Census Bureau staff for work-related purposes.
	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, via Census Bureau VDI, 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.