Version Number: 01-2017

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

Privacy Threshold Analysis
for the
Qualitative Pre-testing & Evaluation Methods (e.g. Focus Groups)

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The Census Bureau's Center for Survey Methodology uses contractor support for a variety of qualitative 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 Threshold Analysis (PTA) covers cognitive interviews and focus groups captured and/or maintained by a third-party contractor. 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 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 researches 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.

The Federal Government Standards offer a framework for security controls to be implemented for information systems in an effort 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 4 – 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

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

The IT systems used for 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 a secure Census Bureau IT system that interconnects with other secure Census Bureau IT systems.

(d) The purpose that the system is designed to serve

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.

(e) The way the system operates to achieve the purpose

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.

(f) A general description of the type of information collected, maintained, use, or disseminated by the system

Focus groups and qualitative interviews collect general information on opinions, attitidudes and understanding of production Census Bureau data collection instruments. These data are used to evaluate and improve Census Bureau surveys and censuses.

(g) Identify individuals who have access to information on the system

Only Census Bureau researchers and SSS contractors with a business need to know will have access to the information on the system.

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

Information in the IT system will be retrieved by aggregate dataset groups, not by personal identifiers, for example interview number assigned to a set, focus group number assigned to a set, etc.

(i) 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.

Questionnaire:

1. What is the status of this information system?

__x__ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_x___ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__x__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__x__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__x__ DOC employees
__x__ Contractors working on behalf of DOC
__x__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_x___ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__x__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Qualitative Pre-testing & Evaluation Methods (e.g. Focus Groups) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Qualitative Pre-testing & Evaluation Methods (e.g. Focus Groups) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Jennifer Hunter Childs

Signature of ISSO or SO: JENNIFER CHILDS Digitally signed by JENNIFER CHILDS Date: 2018.08.22 13:40:46 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Timothy Ruland

Signature of ITSO: TIMOTHY RULAND Digitally signed by TIMOTHY RULAND Date: 2018.09.04 07:40:07 -04'00' Date: _____

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO: Kevin Smith Date: 9/26/18

Name of Business Authorizing Official (AO): John Eltinge

Signature of AO: _____ Date: 9/28/2018

Name of Bureau Privacy Officer (BPO): Byron Crenshaw Byron Crenshaw

Signature of BPO: _____ Date: 9/26/18