Template Version Number: 01-2021

U.S. Department of Commerce
Census Bureau

Privacy Threshold Analysis
for the
Associate Director for Economic Programs (ADEP)
Innovation and Technology Office (ITO)

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau ADEP ITO Applications

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

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for ADEP ITO systems. 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. Questions and guidance regarding this PTA should be referred to the Census Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

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 ADEP ITO system is comprised of major applications that:

- Provide users the ability to design how paper, internet, computer assisted, and/or telephone assisted instruments should appear (e.g., what questions should be asked, when they should be asked, etc.), and provide users the ability to design how their respondent materials should appear (e.g., define the contents).
- Perform paper-based data collection activities that facilitates the Batching, Scanning, Registration, Interpretation, Quality Control Measurement, Error Containment, as well as an Exception Review process while providing scanned digital images of respondent questionnaires in real time.
- Provide Census Bureau analysts secure access to the 2010 and 2020 census data and the digital images of the questionnaires from which the data were captured to support comprehensive and accurate reviews, evaluations, and research.
- Provide survey operational control functionality needed to support field, internet, and telephone data collection operations.

Address the following elements:

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

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

b) System location

ADEP ITO system is hosted within the following locations:

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

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

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

d) The purpose that the system is designed to serve

ADEP ITO system is designed to:

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

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

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

• Provide survey operational control functionality needed to support field, internet, and telephone data collection operations. Operational control functionality includes manages cases, regardless of mode and case type, by creating operational workloads, pushing these cases to the data collection instruments, and tracking key status and events for each case during the data collection lifecycle.

e) The way the system operates to achieve the purpose

ADEP ITO system operates by:

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

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

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

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

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

ADEP ITO system stores personally identifiable information (PII)/business identifiable information (BII) such as name, address, business name, email address, telephone number, etc.

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

Individuals with access to the ADEP ITO information system are authorized Census employees or contractors.

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

Information within the ADEP ITO system is retrieved by authorized users using internal web interfaces, application programming interfaces, secure databases, and managed file transfer servers. Information contained within the system is not available to the public. Only authorized Census Bureau federal employees and contractors with a need-to-know have access to the system. Data is searchable/retrievable by PII.

i) How information is transmitted to and from the system

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

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ 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.*

_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. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

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.*

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

__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.)."

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

____ 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
____ Other Federal Government personnel
_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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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 ADEP ITO applications 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 [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Christine Moseley Office: Innovation and Technology Office Phone: 301-763-7194 Email: christine.j.moseley@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CHRISTINE MOSELEY Digitally signed by CHRISTINE MOSELEY Date: 2022.12.14 10:33:37 -05'00' Date signed:	**Chief Information Security Officer** Name: Beau Houser Office: Office of Information Security Phone: 301-763-1235 Email: beau.houser@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2022.12.19 18:15:49 -05'00' Date signed:
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: Byron.Crenshaw@Census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.01.03 10:30:08 -05'00' Date signed:	**Authorizing Official** Name: Luis J. Cano Office: Office of the Chief Information Officer Phone: 301-763-3968 Email: luis.j.cano@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2022.12.20 11:07:36 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: Byron.Crenshaw@Census.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.01.03 10:28:01 -05'00' Date signed:	**Business Authorizing Official** Name: Nick Orsini Office: Associate Directorate of Economic Programs Phone: (301) 763-6959 Email: Nick.Orsini@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: NICK ORSINI Digitally signed by NICK ORSINI DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Bureau of the Census, cn=NICK ORSINI, 0.9.2342.19200300.100.1.1=13001000014152 Date: 2022.12.28 10:38:02 -05'00' Date signed: