Privacy Threshold Analysis
for the
CEN36
Integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), and MOJO Enhanced Operational Control System
U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/Integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), and MOJO Enhanced Operational Control System

Unique Project Identifier: 006-00402100

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 and its purpose 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).

iCADE (integrated Computer Assisted Data Entry) System scans and keys data from demographic, economic, and decennial census questionnaires received by mail from respondents. The iCADE reports module provides real-time status information for survey sponsors. CEN36 stores PII/BII information such as name, address, business name, email address, telephone number etc.

CIRA (Census Image Retrieval Application) contains the 2010 Decennial Data Capture Images as well as the edited and unedited data. This application is used by survey analysts to review anomalies in the 2010 Data for a specified task. This application has an extensive approval process in order for any individual to access or review data. Users only have access to view approved images and data based on an approved business case.

MOJO Enhanced Operational Control System will provide optimized routing and assignment attempts for Census Bureau enumerators. It will also provide data to managers so they can monitor operations performance.

Questionnaire:

1. 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.

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

X This is an existing information system in which changes do not create new privacy risks. 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.

   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

   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.”

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

___ DOC employees
___ Contractors working on behalf of DOC
___ 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?

___ 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.

___ 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 CEN36 system 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.

Name of Information System Security Officer (ISSO) or System Owner (SO):

__________________________
Peter Hoang

Signature of ISSO or SO: __________________________ Date: 03/28/2017

Name of Chief Information Security Officer (CISO):

__________________________

Signature of CISO: __________________________ Date: 3/29/17

Name of Authorizing Official (AO):

__________________________

Signature of AO: __________________________ Date: 4/11/17

Name of Bureau Chief Privacy Officer (BCPO):

__________________________

Signature of BCPO: __________________________ Date: 4/5/17