Version Number: 01-2020

U.S. Department of Commerce
Census Bureau

Privacy Threshold Analysis
for the
Associate Director for Economic Programs (ADEP)
Innovation and Technology Office (ITO) (CEN36)

U.S. Department of Commerce Privacy Threshold Analysis

Integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), Content Meta Data (COMET), MOJO (Optimizer, Recruiting Dashboard, Browse Living Quarters, Hermes) (CEN36)

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 CEN36 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 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).

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

COMET, CIRA, iCADE, and MOJO are major applications.

b) System location

COMET, Census Bureau's Bowie Computer Center (BCC).
CIRA, National Processing Center (NPC) in Jeffersonville, Indiana.
iCADE, National Processing Center (NPC) and Paper Data Capture Center in Jeffersonville, Indiana, and Phoenix Arizona Paper Data Capture Center.
MOJO, Census Bureau's Bowie Computer Center (BCC) and AWS GovCloud environment.

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

COMET and iCADE interconnect to support the delivery of question content and metadata to create an iCADE master template for data capture scan testing and production processing. COMET provides the necessary metadata to Centurion (CEN15) to render electronic instruments.

The iCADE system provides case status information to ATAC (Automated Tracking and Control System) in CEN06 National Processing Center. The iCADE system will pass paper response data and event data to Enterprise Collection and Survey Enabling Platform (ECaSE) system in CEN05 which performs sufficiency checks, and adds post processing variables for subsequent processing by downstream systems. PEARSIS will deliver data from the Administrative Records T13 Composite file, which iCADE will use to improve the Optical Character Recognition (OCR) match rate.

MOJO will also receive contact strategy information from the Research & Methodologies Directorate and Non-Response Follow Up (NRFU) files from the Decennial Census, CEN08 authorization boundary. This strategy information includes respondent data from ECaSE and enumerator information from DAPPS for optimization of workload assignments. MOJO will receive one-directional exchange of data from the Census Data Lake (CDL) in CEN18, consisting of Workload, Event, Paradata, Response, and Sample Delivery File (SDF) data for the Browse Living Quarters (BLQ) application. MOJO is hosted by a Federal Risk and Authorization Management Program (FedRAMP) approved Cloud Service Provider (CSP).

CEN36 shares information with the following internal Census Bureau IT systems: CEN05 ECaSE, CEN06 National Processing Center (NPC) systems, CEN07 Geography, CEN08 Decennial, CEN15 Centurion, CEN18 CDL, CEN21 DAPPS.

d) The purpose that the system is designed to serve

COMET is a major application for the long-term solution to standardize input requirements across modes of data collection including metadata across surveys and Census in support of dissemination.

CIRA (Census Image Retrieval Application) system 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 and are Census employee/contractors.

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.

MOJO Optimizer operational control system and the Recruit Dashboard provide optimized routing and assignment attempts for Census Bureau enumerators. The Recruiting Dashboard

provides data to managers so they can monitor operations performance by providing insight into the progress of recruiting operations at lower levels of geography (tract). MOJO allows users to search housing units in the enumeration universe and display potentially dangerous addresses using the Browse Living Quarters (BLQ) application, and the Hermes application to generate management reports.

e) The way the system operates to achieve the purpose

COMET – provides a repository for content metadata, a user interface for managing content, producing record layouts and data dictionaries, and creating and approving Office of Management and Budget (OMB) Pre-submission and Clearance Packages.

CIRA – provides a query browser that allows analysts to review data and its associated images for a specific, approved business case.

iCADE - receives paper questionnaires from respondents via the United States Postal Service (USPS) where the staff at the National Processing Center (NPC) opens the envelopes and removes the forms. The forms are scanned by iCADE scanner operators and respondent data is captured in an automated fashion with use of Optical Character Recognition (OCR) and Optical Mark Recognition (OMR). Any respondent data that is not captured via OMR or OCR is then sent to an iCADE keyer for capture. All respondent data is held in a script file and then transferred to the survey sponsor owner via a secured connection.

MOJO – receives enumerator information from Decennial Applicant, Personnel and Payroll System (DAPPS), contact strategy information from the Research & Methodologies Directorate, and Non-response follow-up (NRFU) workload from the Enterprise Collection and Survey Enabling Platform (ECaSE) system. MOJO will take the information and create daily workload assignments that will be pushed back to ECaSE. MOJO will also receive workload, event, ISR instrument paradata, response, and SDF for all 2020 Census operations from the Census Data Lake (CDL).

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

CEN36 stores PII/BII information such as name, address, business name, email address, telephone number etc. COMET does not store PII/BII.

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

Individuals with access to the CEN36 information systems are authorized Census Employees or Contractors.

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

COMET – provides a software browser user interface for accessing questionnaire information contained within the repository. COMET will allow for assignment of user roles with unique permissions. These roles are either context independent (across various surveys) or context dependent (specific to a survey).

CIRA – provides a software browser user interface for reviewing data and associated images. User access to the images and supporting variables is strictly controlled. Requests for project approval and user access is on a case-by-case basis.

iCADE - provides a software user interface data capture solution for paper-based data collection operations, real-time reports on workflow, survey processing completeness, and accuracy and performance metrics for all automatic and clerical processes. It is only accessible to select users that have had their login credentials validated against the Census LDAP.

MOJO – The Optimizer application provides no end user access. Optimizer information within MOJO is accessed by system administrators via web services for the purpose of monitoring generation of workload assignments. The MOJO BLQ application will provide approved Area Census Office (ACO), Regional Census Office (RCC), and headquarters (HQ) staff the ability to search for housing units in the enumeration universe during the 2020 Census using the same protocols as currently deployed within the Recruiting Dashboard.

i) How information is transmitted to and from the system

COMET – Information transmission to and from the COMET system is accomplished via Web Services using the COMET Service Registry in XML format. COMET also uses JSON to deliver data to Centurion, and has a direct DB link for iCADE.

CIRA – The Census Image Retrieval Application (CIRA) is limited to image searching and viewing. No data is transmitted to the end users. CIRA does not permit users to upload, modify or delete data or form images within the CIRA database.

iCADE – Information transmitted to and from iCADE is accomplished via secure protocols in XML format. Information output files for the sponsors can be created in a variety of formats including ASCII, EXCEL, TXT, and Oracle.dmp.

MOJO – Information transmitted to and from MOJO is accomplished via Java Database Connectivity (JDBC) and secure file transfer mechanisms.

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): New MOJO application functionality; Recruiting Dashboard, BLQ and Hermes migrated to AWS GovCloud in 2018/2019.					

____ 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 (version 01-2015 or 01-2017). *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 01-2019 or later). *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.