Version Number: 01-2015

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

Privacy Impact Assessment
for IT System: CEN36
Integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), and MOJO Enhanced Operational Control System

Reviewed by: Rolig Bacho 2/3/17, 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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.07.25 13:47:50 -04'00'

5/18/2017

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer — Date

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/CEN36/integrated Computer Assisted Data Entry (iCADE), Census Image Retrieval Application (CIRA), and MOJO Enhanced Operational Control System

Unique Project Identifier: 006-00402100

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system

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.

(b) a description of a typical transaction conducted on the system

The Census Bureau 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 such as Master Control.

CIRA – provides a query browser that allows analysts to review data and its associated images for a specific approved business case. CIRA only allows users access to the data and images associated with the approved business case.

MOJO – will receive 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 Decennial Census. It will take the information and create daily workload assignments that will be pushed to a hand-held device for data collection. As the enumerator is collecting data, the data will be pushed from the hand-held device back to MOJO for real time reporting.

(c) any information sharing conducted by the system

The iCADE system provides case status information to ATAC (Automated Tracking and Control System) in CEN06 National Processing Center.

MOJO will push information to Census Operations Mobile Platform for Adaptive Services and Solutions (COMPASS) (a handheld device application) that is within the CEN05 IT system boundary and DAPPS.

MOJO will also receive contact strategy information from the Research & Methodologies Directorate and Non-Response Follow Up (NRFU) files from Decennial Census information which is inside of the CEN08 boundary. This strategy information includes respondent data from COMPASS and enumerator information from DAPPS.

CEN36 shares information with the following additional internal Census Bureau IT systems: CEN07 Geography, CEN08 Decennial, CEN13 Center for Economic Studies, CEN15 Centurion, and CEN18 Enterprise Applications.

(d) a citation of the legal authority to collect PII and/or BII

The legal authorities to collect PII/BII for the CEN 36 IT systems are: 13 U.S.C. Sections 8(b), 131, 132, 141,182, 193, 196, 26 U.S.C 6103(j), 5 U.S.C. 301, and 44 U.S.C. 3101.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is 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):					

_X_ This is an existing information system without changes that do not create new privacy risks.

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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

Other Information (specify)
Paradata

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		Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	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 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		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	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			
To determine eligibility		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		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For statistical purposes (i.e., Censuses/Surveys)			

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).

PII/BII is collected from the public for statistical purposes and from Census Bureau employees/contractors.

The iCADE System collects data from respondent paper questionnaires used by the demographic, economic, and decennial census programs. The data is provided to each survey sponsor and is used for statistical survey dissemination of data to other agencies and the public. iCADE captures data for approximately 40 surveys/projects annually.

The CIRA System contains the data and images from the Decennial Census. This system allows analysts to do data review as well as research for decisions related to the 2020 Census. This system is for internal use only and is in reference to members of the public.

The MOJO System is currently being built/enhanced to support Decennial site tests. The system is the operational control system receiving data from the field hand-held COMPASS device and then providing it to the sponsor. MOJO also includes some Census Bureau employee/contractor information.

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 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: CEN36 shares information with the following internal Census Bureau IT systems: CEN07 Geography, CEN08 Decennial, CEN13 Center for Economic Studies, CEN15 Centurion, and CEN18 Enterprise Applications. CEN36 receives information from CEN01 and CEN05. CEN36 uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (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, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems. Census also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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.)*

X	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: http://www.census.gov/about/policies/privacy/privacy-policy.html_____.	
	Yes, notice is provided by other means.	Specify how:
	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: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII for some questions.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Some Census Bureau surveys are mandatory as required by 13 U.S.C. Individuals are informed of this by one of the following: Privacy Act Statement upon login, letter, interview, or during data collection.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII for some questions there for they are not consenting to particular uses of their PII/BII.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Some Census Bureau surveys are mandatory as required by 13 U.S.C. There for they not have the opportunity to consent to particular uses of their PII/BII.

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: If the Census Bureau contacts the respondent for an update then the respondent can provide the updated information. For some Census Bureau surveys, individuals have the opportunity to provide updates to PII data within the submitted survey or survey website.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For surveys covered under SORNs Census-4 and Census-5 there are no access & contest requirements since the data is collected for statistical purposes.

Section 8: Administrative and Technological Controls

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

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	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: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 28, 2016 ☐ 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 or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 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 (POAM).
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 ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify): Publications are approved by the disclosure review board.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/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 Information technology 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 has a current authority to operate (ATO) and goes through 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.

Section 9: Privacy Act

9.1 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 and number *(list all that apply)*: Yes, this system is covered by an existing system of records notice. Provide the system name and number: Census - 5, Decennial Census Program: https://www.federalregister.gov/documents/2014/04/21/2014-08993/privacy-act-system-of-records COMMERCE/Dept-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons: https://www.gpo.gov/fdsys/pkg/PAI-2013-COMMERCE/xml/PAI-2013-COMMERCE.xml#dept1
X	Yes, a SORN has been submitted to the Department for approval on (date). Census - 3, Demographic Survey Collection (Census Bureau Sampling Frame) submitted on 7/22/16 Census - 4, Economic Survey Collection submitted on 8/24/16 Census - 7, Demographic Survey Collection (non-Census Bureau Sampling Frame) submitted on 7/22/16
	No, a SORN is not being created.

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: N1-29-98-1 N1-029-05-2 N1-029-10-3 NC1-29-82-4 N1-029-10-4 NC1-29-82-4, Item 56 N1-29-92-1, Item D or 12c DAA-0029-2013-0004
	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:
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	X
Degaussing		Deleting	X
Other (specify):			

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

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.

	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII/BII 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 collection is for all U.S. housing units, therefore, a serious or substantial number of individuals would be affected if there was loss, theft, or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII/BII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII in this IT system is protected under the authority of 13 U.S.C 9.
X	Access to and Location of PII	Provide explanation: The PII/BII is located on computers (including laptops) and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know including the Census Bureau geographic program area, regional offices, and survey program offices, etc. Access is only allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities.
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.