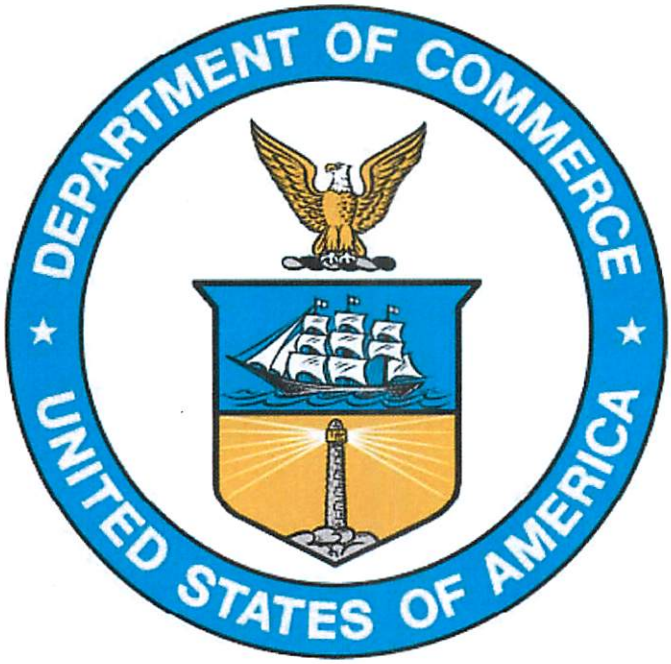
Version Number: 01-2017

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



Privacy Threshold Analysis
for the
CEN08 Decennial

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/CEN08 Decennial

Unique Project Identifier: 006-000400400

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).

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

CEN08 Decennial consists of both major applications and general support systems that collect, maintain and process, and/or disseminate data collected from decennial census respondents and decennial census personnel:

Major Applications: In accordance with NIST and OMB Circular A-130 Appendix III, a major application is an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access or modification of the information in the application.

CEN08 Decennial manages the development and implementation of major decennial census applications utilized by the Decennial Census Program in order to produce statistics. These applications process response data from census tests and 2020 Census operations, and perform quality assurance mechanisms for various census operations.

The CEN08 Decennial IT system monitors the cost, schedule, and technical performance milestones for each software system or application utilized for decennial census purposes. The CEN08 IT system manages the development and implementation of software and systems necessary to support collection, processing, and tabulation of census data.

Major applications that collect, maintain, process, and/or disseminate PII include:

Control and Response Data System (CaRDS) - CaRDS provides sample design and Universe

determination for the Decennial Census.

Sampling, Matching, Reviewing, and Coding System (SMaRCS) - SMaRCS supports quality control operations designed to determine whether field listers and enumerators are using validated procedures and collecting accurate data. SMaRCS facilitates quality control operations by providing a mechanism for selecting quality control samples, validating production interview data against administrative records sources, and by providing a tool for clerical matching to compare the production interview data against re-interview (RI) data.

Decennial Response Processing System (DRPS) - DRPS provides Autocoding, Clerical coding, Data editing and imputation for the Decennial post data collection response processing. Additionally, it creates Decennial Response Format (DRF), Census Unedited File (CUF) and Census Edited File (CEF) files.

Disclosure Avoidance System (DAS) – DAS applies privacy controls to microdata in the data flow from the Census Edited File (CEF) to the Microdata Detail File (MDF). The privacy controls assure that there is no direct mapping between individual records in the CEF to individual records in the MDF.

SAS Foundation – SAS Foundation provides Sampling Criteria, Contact Strategies and Sample for re-interviews, manages the 2020 Experiments Program, and verifies the Sample Design File (SDF).

Production Environment for Administrative Records Staging, Integration and Storage (PEARSIS) –PEARSIS manages Administrative Records and services associated with these records. Services include preparing, storing, and distributing for Census production (PROD) operations.

Self-Response Quality Assurance (SRQA) - Self-Response Quality Assurance (SRQA) identifies fraudulent responses either real-time or post data collection.

Post-Enumeration Survey (PES) – PES includes the Processing and Control System (PCS) which performs automatic matching, workload control and sampling for Coverage Measurement, Imputation and Estimation System which performs the imputation and estimation for Coverage Measurement, and Clerical Match and Map Update (CMMU) which performs clerical matching activities and map spot updates for Coverage Measurement. The Coverage Measurement program will provide estimates of net coverage error and components of census coverage for housing units and people in housing units.

Some examples of the information collected, maintained, processed, and/or disseminated within the major applications are names, addresses, gender, age, date of birth, race, email, education, telephone number and salary. Refer to Section 2: Information in the System below for a complete listing of information contained within the major applications.

General Support System: In accordance with NIST and OMB Circular A-130 Appendix III; a general support system is an interconnected set of information resources under the same

direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

General support systems that collect, maintain, process, and/or disseminate PII include:

Third Party Fingerprinting – The Third Party Fingerprinting solution is an external system managed by Indrasoft. The U.S. Census Bureau (USCB) employs hundreds of thousands of temporary workers to perform data collection activities via a non-competitive Schedule A hiring authority from the Office of Personnel Management (OPM) in support of the Decennial Census testing in Fiscal Year (FY) 2018 and 2020 Census. As part of the recruitment and security process, the USCB requires that these selectees undergo fingerprinting to determine their suitability for employment. In addition, contractors that provide services in support of the 2020 Decennial Census, such as Census Questionnaire Assistance (CQA) contractor candidates, will be fingerprinted. To support fingerprinting for the 2020 Census, the USCB will use the Third Party Fingerprinting solution to capture and transmit fingerprints to USCB and conduct identity proofing for these temporary hires and contractors.

Recruiting and Assessment (R&A) – R&A is an external system that is managed by Cornerstone On Demand. R&A provides capabilities for applicant recruiting, learning management system (LMS) and the applicant pre-selection assessment process for temporary hires and contractors. Information collected includes Name, Social Security Number, Birthdate, Address and Work History. Refer to Section 2: Information in the System below for a complete listing of information contained within R&A.

Decennial Physical Access Control System (DPACS) is an internal managed badging solution where all 2020 Census Enumerators and Census Field Supervisors (CFS) that will be hired to work at Area Census Offices (ACOs) and at Regional Census Centers (RCCs) are issued, in a timely manner for all relevant operations, a Census ID badge with the employee's photo and name printed on it, in conformance to a template provided by the Office of Security (OSY), for stateside (including Remote Alaska), DC, and Puerto Rico; and for the Census of Island Areas.

2020 Print Vendor – The 2020 Print Vendor provides the majority of printing and mailing services for the 2020 Census. The 2020 print vendor, RR Donnelley, will print surveys on physical paper and address envelopes for delivery to survey recipients. Information shared with the 2020 print vendor includes name and address information.

b) System location

Major Applications: All major applications and backups are hosted within Bowie Computer Center (BCC) located in Bowie, Maryland and/or AWS GovCloud (US-East) Region located in the Northeastern part of the United States.

General Support Systems:

Third Party Fingerprinting – AWS U.S. East/West located in US East (Ohio), US East (N. Virginia), US West (N. California), and US West (Oregon) and physical fingerprinting capture sites across the United States.

R&A - Unified Talent Management Suite (CUTMS) Cloud located in El Segundo, CA and Ashburn, VA.

DPACS Badging - Area Census Offices (ACOs) and Regional Census Centers (RCCs).

2020 Print Vendor – Headquarters in Chicago, Illinois.

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

Major Applications – Interconnects internally with systems within Field CEN05, Geospatial Services CEN07, Demographic Surveys CEN11, Census Data Lake (CDL) CEN18, Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI) CEN19, Decennial Applicant, Personnel and Payroll Systems (DAPPS) CEN21, American Community Survey CEN30, and Economic Programs, Associate Director for Economic Programs (ADEP) CEN36.

General Support Systems:

Third Party Fingerprinting – Interconnects with Census Hiring and Employment Check System (CHEC) CEN21 and DPACS Badging.

R&A – Interconnects with DAPPS CEN21.

DPACS Badging - Interconnects with DAPPS CEN21 and Third Party Fingerprinting.

2020 Print Vendor – No direct interconnections will be established with the 2020 Print Vendor.

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

The CEN08 DITD provides updates and unit (e.g., a home, a building, or miscellaneous structure) status information to various divisions within the Census Bureau that maintain address information (e.g., street addresses, and status and control information for households and other living quarters). In addition, CEN08 systems confirm receipt of response data. They also provide validation and acknowledgment of the data received from various IT systems.

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

Major Applications - Process response data from census tests and 2020 Census operations, and perform quality assurance mechanisms for various census operations. Data collection is used to produce statistics.

General Support Systems:

Third Party Fingerprinting - To support fingerprinting for the 2020 Census, the USCB will use the Third Party Fingerprinting solution to capture and transmit fingerprints to USCB and conduct identity proofing for temporary hires and contractors (selectees). These selectees will provide their fingerprints at one of the Third Party Fingerprinting physical capture sites.

R&A - Temporary hires and contractors looking to support the 2020 Census submit their job applications through the R&A system. R&A securely delivers the submitted application data and associated attachments to DAPPS for processing and selecting.

DPACS Badging – DPACS Badging activities include badge creation and management system for field badges (CFS., Listers and Enumerators) for the 2020 Census. All 2020 Census non-PIV badge creation will use this system.

2020 Print Vendor – The 2020 Print Vendor is contracted to print and address internet invitations, reminder cards, and questionnaire packages, mail invitations, reminder cards, and questionnaire packages.

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

Some examples of the information collected, maintained, processed, and/or disseminated from respondents are names, addresses, gender, age, date of birth, race, email, education, telephone number and salary.

Some examples of the information collected, maintained, processed, and/or disseminated from decennial census personnel are fingerprints, names, address, date of birth, social security number and work history.

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

Individuals who have access to information on the system include approved Census Bureau federal employees and contractors with a need-to-know.

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

Information in the CEN08 DITD systems are retrieved by using PII information by authorized users using internal web applications, secure databases, and managed file transfer servers. Authorized Census Hiring Employment Check (CHEC) users pull selectee

fingerprint files from the Third Party Fingerprinting solution and forward to the FBI for processing.

Information contained within the major applications and general support systems are not available to the public. Only authorized Census Bureau federal employees and contractors with a need-to-know have access to the applications. These authorized users interface with the information contained within the applications and systems using authorized internal web applications, file servers, and/or databases that are protected with a multi-layer security approach.

i) How information is transmitted to and from the system

Information is transited to and from the major applications using either the Census Bureau Enterprise Service Bus (ESB) via the service oriented architecture (SOA) suite and/or secure point-to-point connections.

General Support Systems:
Information is transferred to and from Third Party Fingerprinting, R&A, DPACS Badging using the Census Bureau Enterprise Service Bus (ESB) via the service oriented architecture (SOA) suite.

Information is transferred to the 2020 Print Vendor using a secure point-to-point connection.

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.*

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): Third Party Fingerprinting will capture fingerprints for selectees (i.e. sworn status temporary hires or contractors) to conduct 2020 Census operations on behalf of the U.S. Census Bureau. Selectee fingerprints are processed and submitted to the FBI in support of conducting background investigations. Survey respondent fingerprints are not collected and no survey respondent data is submitted to the FBI. Photographs are captured for Census ID badges by the DPACS Badging system for Census Enumerators and Census Field Supervisors (CFS) that will be hired to work at Area Census Offices (ACOs) and at Regional Census Centers (RCCs). The Census ID badge includes the employee's photo and name printed on it. Survey respondent photographs are not collected.					

____ 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 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 CEN08 Decennial 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 System Owner (SO): Phani-Kumar Atri Kalluri

Signature of or SO: _____ Date: 5/1/19

Name of System Owner (SO): Luis Cano

Signature of or SO: _____ Date: 5/1/19

Name of Chief Information Security Officer (CISO): Jeffery Jackson

Signature of ITSO: _____ Date: 2 MAY 2019

Name of Technical Authorizing Official (TAO): Kevin B. Smith

Signature of TAO: _____ Date: 4/30/19

Name of Business Authorizing Official (BAO): Albert E. Fontenot Jr.

Signature of BAO: _____ Date: 5/1/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: _____ Date: 4/30/19