

**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: [Number]

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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 applications and systems that collect, maintain and process, and/or disseminate data collected from decennial census respondents and decennial census personnel.

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

Applications and systems 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.

Decennial Response Processing System (DRPS) - DRPS provides Auto-coding, 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.

Decennial Budget Integration Tool (DBiT) – DBiT is used by the Decennial Budget Office (DBO) to perform ongoing cost estimation, budgeting, budget planning, and budget execution management functions required to prepare and execute the Census 2020.

Decennial Physical Access Control System (DPACS) Badging - DPACS Badging is an internal managed badging solution where all 2020 Census Enumerators and Census Field Supervisors (CFS) that are hired to work at Area Census Offices (ACOs) and at Regional Census Centers (RCCs) are issued, in a timely manner for 2020 field 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.

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.

Infrastructure Services – Infrastructure Services includes hardware and software used to manage and support 2020 Decennial applications and systems.

Intelligent Mail Barcode (IMb) Postal Tracking System (IPTS) – IPTS provides the capability to capture United States Postal Service (USPS) IMb tracing data for all IMb'd Census Bureau mail pieces. IPTS collects a variety of USPS mail tracing data including incoming USPS questionnaire scans, outgoing USPS mail piece scans, Undelivered as Addressed (UAA) information, and Secure Destruction confirmations. The use of this information is to effectively manage field and mailing workloads (i.e., if the Census Nonresponse Follow-up (NRFU) field operation becomes aware of an incoming questionnaire associated with an address slated for field follow-up).

Intelligent Telecommunications Management System (ITMS) - ITMS provides asset tracking and reporting for mobile devices used for 2020 Decennial operations.

Network Infrastructure – Network Infrastructure includes hardware and software used to manage the connectivity and communication across 2020 Decennial applications and systems.

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.

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.

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 provides estimates of net coverage error and components of census coverage for housing units and people in housing units.

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.

Self-Response Quality Assurance (SRQA) - The purpose of the Self-Response Quality Assurance (SRQA) operation is the identification of suspicious self-responses submitted during the 2020 Census. The SRQA operation contains automated and interactive analyses to identify suspicious individual or groups of self-responses. In addition, there is a field portion of the SRQA operation to assist in assuring the quality of self-responses. SRQA outcomes are reported to 2020 Census post-processing.

Third Party Fingerprinting (TPF) – The TPF 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, temporary hires that provide services in support of the 2020 Decennial Census, such as Census Questionnaire Assistance (CQA), are fingerprinted. To support fingerprinting for the 2020 Census, the USCB uses the Third Party Fingerprinting solution to capture and transmit fingerprints to the Federal Bureau of Investigation (FBI) via USCB and conduct identity proofing for these temporary hires.

2020 Print and Mailing Vendor – The 2020 Print and Mailing Vendor provides the majority of printing and mailing services for the 2020 Census. This includes printing Census questionnaires on physical paper and address envelopes for delivery to households. Information shared with the 2020 Print and Mailing Vendor includes address information.

(b) System location

CaRDS, DRPS, DBiT, DAS, Infrastructure Services, IPTS, ITMS, Network Services, SMaRCS, SAS Foundation, PEARSIS, PES, and SRQA are hosted and managed within the Bowie Computer Center (BCC) located in Bowie, Maryland and/or AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions located in the Eastern and Northwestern parts of the United States.

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

R&A - Unified Talent Management Suite (CUTMS) Cloud located in data centers within the United States.

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.

2020 Print and Mailing 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)

CaRDS, DRPS, DBiT, DAS, DPACS Badging, Infrastructure Services, IPTS, ITMS, Network Services, SMarCS, SAS Foundation, PEARSIS, PES, R&A, TPF and SRQA interconnects internally with systems within the Census Bureau which include 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.

2020 Print and Mailing Vendor – No direct interconnections are established with the 2020 Print and Mailing Vendor.

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

The main purpose of CEN08 is to for statistical purposes including the censuses and surveys. CEN08 is also used for human resource purposes, which includes hiring for the 2020 Census.

(e) The way the system operates to achieve the purpose(s)

CaRDS, DRPS, DBiT, DAS, Infrastructure Services, IPTS, ITMS, Network Services, SMarCS, SAS Foundation, PEARSIS, PES, and SRQA support the collection, monitoring, and processing 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.

DPACS Badging – DPACS Badging activities include badge creation and management system for field badges (CFS, Listers and Enumerators) for the 2020 Census field operations.

R&A - Temporary hires looking for employment for 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.

Third Party Fingerprinting - To support fingerprinting for the 2020 Census, the USCB uses the Third Party Fingerprinting solution to capture and transmit fingerprints to the FBI via USCB and conduct identity proofing for selectees. These selectees provide their fingerprints at one of the Third Party Fingerprinting physical capture locations.

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

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

CaRDS, DRPS, DBiT, DAS, Infrastructure Services, IPTS, ITMS, Network Services, SMaRCS, SAS Foundation, PEARSIS, PES, and SRQA - The PII collected, maintained, and/or disseminated by these applications and systems is in reference to members of federal employee/contractors and the public. Federal employee/contractor information is maintained to support access controls and audit logging activities. Data collection from the public is used to produce national statistical information.

DPACS - The PII collected, maintained, and/or disseminated by DPACS Badging is in reference to temporary hires. DPACS Badging generate field badges that includes name and photograph of CFS, Listers, and Enumerators in support of the 2020 Census.

R&A - The PII collected, maintained, and/or disseminated by R&A is in reference to temporary hires. Temporary hires 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 CEN21 for processing and selecting.

TPF - The PII collected, maintained, and/or disseminated by Third Party Fingerprinting is in reference to temporary hires. Third Party Fingerprinting is capturing selectee fingerprint data on behalf of the U.S Census Bureau to hire selectees to help conduct the 2020 Census operations. The vendor does not directly submit the fingerprint information to the FBI, rather the information is securely sent to the U.S Census Bureau for processing and submission to the FBI. The third party vendor is mandated to only utilize FedRAMP authorized solutions.

2020 Print and Mailing Vendor - The PII collected, maintained, and/or disseminated by the 2020 Print and Mailing Vendor is in reference to members of the public. Address information is needed to print census questionnaires on physical paper and address envelopes for delivery to household recipients.

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

U.S Census Bureau government employees and contractors

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

Information in CEN08 Decennial applications and systems are retrieved by using PII information identified in Section 2 below by authorized users using internal web applications, secure databases, and managed file transfer servers.

Information contained within the applications and 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 as described in Section 5.2 below.

(i) How information is transmitted to and from the system

Information is transmitted to and from CaRDS, DRPS, DBiT, DAS, DPACS Badging, Infrastructure Services, IPTS, ITMS, Network Services, SMarCS, SAS Foundation, PEARSIS, PES, R&A, TPF and SRQA using either the Census Bureau Enterprise Service Bus (ESB) via the service oriented architecture (SOA) suite, application program interfaces (API) and/or secure point-to-point connections.

Applicants' fingerprints are captured on TPF physical sites which is uploaded to the authorized AWS U.S. East/West. Files are encrypted and transferred using the service-oriented architecture (SOA) via the Enterprise Service Bus (ESB), which then sends it over to CHEC within the U.S Census Bureau. The Enterprise Service Bus is a configuration-based, policy-driven enterprise service bus. It provides highly scalable and reliable service-oriented integration, service management, and traditional message brokering across heterogeneous IT environments. It combines intelligent message brokering with routing and transformation of messages, along with service monitoring and administration in a unified software product.

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

CaRDS, DRPS, DBiT, DAS, DPACS Badging, Infrastructure Services, IPTS, ITMS, Network Services, SMarCS, SAS Foundation, PEARSIS, PES, R&A, TPF and SRQA shares information internally with systems within the Census Bureau which include 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.

In addition, fingerprints captured by TPF for potential new hires, are sent directly to the FBI via USCB to process and assist with decennial hiring practices.

2020 Print and Mailing Vendor – Address files are transmitted to the 2020 Print and Mailing Vendor.

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):			

- 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.*
- 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). *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 01-2017 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. *(Check all that apply.)*

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

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.

No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

DOC employees

National Institute of Standards and Technology Associates

Contractors working on behalf of DOC

Other Federal Government personnel

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.

R&A - Temporary hires looking to support the 2020 Census submit their job applications through the R&A system. Temporary hire social security numbers collected as part of the employment application process per OPM. Census respondent social security numbers are not

collected. No other applications or systems within CEN08 collect the public's social security numbers. R&A also collects Alien Registration information as part of the job application process and direct deposit information as part of the on-boarding process.

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?

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.

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, 4c, and/or 4d 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.

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): Barbara M. LoPresti

Signature of or SO: Barbara LoPresti Digitally signed by Barbara LoPresti
Date: 2020.06.30 14:27:15 -04'00' Date: _____

Name of System Owner (SO): Luis Cano

Signature of or SO: LUIS CANO Digitally signed by LUIS CANO
Date: 2020.06.30 15:33:44 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Beau Houser

Signature of CISO: BEAU HOUSER Digitally signed by BEAU HOUSER
Date: 2020.08.05 18:09:15 -04'00' Date: _____

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

Signature of TAO: KEVIN SMITH Digitally signed by KEVIN SMITH
Date: 2020.08.06 12:35:04 -04'00' Date: _____

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

Signature of BAO: Albert E Fontenot Digitally signed by Albert E Fontenot
Date: 2020.08.19 09:31:35 -04'00' Date: _____

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW
Date: 2020.08.20 10:50:47 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW
Date: 2020.08.20 10:51:05 -04'00' Date: _____