



U.S. Department of Justice
Civil Division, Appellate Staff
950 Pennsylvania Ave. NW, Rm. 7511
Washington, DC 20530

Tel: 202-514-4027

VIA CM/ECF

May 3, 2019

Mr. Mark Langer
U.S. Court of Appeals for the
District of Columbia Circuit
333 Constitution Ave. NW
Washington, D.C. 20001

RE: *Electronic Privacy Info. Ctr. v. U.S. Dep't of Commerce*, No. 19-5031 (D.C. Cir.)
(argument scheduled for May 8, 2019)

Dear Mr. Langer:

I write to notify the Court that, on May 2, 2019, the Census Bureau published an updated privacy impact assessment regarding CEN08, a primary information technology system that the Bureau uses to administer the decennial census. Page 8 of the assessment reflects the Bureau's intent to include a citizenship question on the 2020 Decennial Census. The updated assessment is publicly available at www.osec.doc.gov/opog/privacy/Census%20PIAs/CEN08_PIA_SAOP_Approved.pdf, and we have attached a copy to this letter for the Court's convenience.

We would be grateful if you would provide this letter to the members of the panel.

Sincerely,

s/ *Sarah Carroll*

Sarah Carroll
Attorney, Appellate Staff

cc: counsel (via CM/ECF)

Version Number: 01-2017

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



**Privacy Impact Assessment
for the
CEN08 Decennial**

Reviewed by: Byron Crocker (Acting), 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

Kristen Yefeme for Catrina Purvis 5/2/19
 Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

Version Number: 01-2017

U.S. Department of Commerce Privacy Impact Assessment U.S. Census Bureau/CEN08 Decennial

Unique Project Identifier: 006-000400400

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. Please answer each question (a) through (i) separately.

(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

Version Number: 01-2017

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

Version Number: 01-2017

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)

Version Number: 01-2017

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 way the system operates to achieve the purpose(s) identified in Section 4

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.

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.

Version Number: 01-2017

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.

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

Information in the CEN08 DITD 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. 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 as described in Section 5.2 below.

(f) 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.

Applicants' fingerprints are captured on Third Party Fingerprinting physical sites which is uploaded to 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.

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.

Version Number: 01-2017

(g) Any information sharing conducted by the system

Major Applications – Shares information internally within the Census Bureau with Geospatial Services CEN07, Field CEN05, Demographic Surveys, DEMO 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 – Fingerprints of potential new hires are shared between the fingerprinting solution, CHEC, FBI, DPACS Badging, and with private companies hired to process and assist with decennial hiring practices.

R&A – Shares information internally within the Census Bureau with DAPPS CEN21.

DPACS Badging – Shares information internally within Census Bureau DAPPS CEN21 and Third Party Fingerprinting.

2020 Print Vendor – No information sharing is conducted by the 2020 Print Vendor.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The following authorities apply to all of the CEN08 major applications and general support systems:

Title 13, U.S.C. Section 6c

Title 13, U.S.C. Section 141

Title 13, U.S.C. Section 193

44 U.S.C. Section 3101

41 U.S.C. 433(d)

5 U.S.C. 301

5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533

Executive Order 9397

Executive Order 12107

Executive Order 12564

As noted, the Census Bureau's programmatic authority is Title 13 of the U.S. Code. Title 13 provides authority to conduct the Bureau's work in addition to providing strong confidentiality protections. Section 9 of Title 13 not only requires that the Census Bureau maintain the confidentiality of the information it collects from decennial census respondents, but also mandates that the Census Bureau may use such information it collects for statistical

purposes, and the information cannot be used to a respondent’s detriment. The Census Bureau cannot publish data that identifies a particular individual or establishment, because of Title 13.

The Census Bureau leverages its Title 13 authority and obligations in coordination with other federal statutes and mandates for privacy, data security, transparency, and accountability, including the Privacy Act, the E-Government Act of 2002, FISMA, and the Paperwork Reduction Act as well as federal standards and guidance promulgated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

All CEN08 Decennial major applications and general support systems are classified as 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): 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.

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.)*

Version Number: 01-2017

Identifying Numbers (IN)					
a. Social Security	x	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID	x	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): N/A					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Temporary hires and contractors looking to support the 2020 Census submit their job applications through the R&A system. Temporary hire and contractor social security numbers collected as part of the employment application process per OPM. Survey respondent social security numbers are not collected.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender	x	j. Telephone Number	x	p. Military Service	
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): Citizenship (Should the government prevail in pending litigation regarding the reinstatement of the citizenship question, the Census Bureau will include the citizenship question on the 2020 decennial questionnaire.) ¹ The Department of Justice (DOJ) has requested that the 2020 decennial Census collect block-level data regarding citizens of voting age population in order to permit more effective enforcement of the Voting Rights Act. No personally-identifying information will be shared with DOJ or other parties, only deidentified statistical information, like other information shared about survey respondents.					
CEN08 major applications process response data (general personal data as marked above) from census tests and 2020 Census operations, and perform quality assurance mechanisms and analysis for various census operations.					

Work-Related Data (WRD) ²					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address		h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):N/A					

Distinguishing Features/Biometrics (DFB)
--

¹ This privacy impact assessment as a whole addresses the proposed collection of citizenship information. Sections 1, 2, 3, 4, 5, and 6 of this privacy impact assessment address "what information is to be collected," "why the information is being collected," "the intended use of the agency of the information," and "with whom the information will be shared," and are fully applicable to the citizenship question. In particular, Decennial Census response information is protected from unauthorized disclosure under Title 13: the Census Bureau may use decennial responses only for statistical purposes and cannot share data that identifies a particular individual or establishment, even with other agencies. 13 U.S.C. § 9; see also 13 U.S.C. § 8(b). Section 7 addresses "what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared." Section 8 addresses "how the information will be secured." Section 9 addresses "whether a system of records is being created under" the Privacy Act. Sections 10, 11, and 12 of this PIA are also applicable to the citizenship question.

² Temporary hires and contractors looking to support the 2020 Census submit their job applications through the R&A system. Temporary hire and contractor work information as marked above are collected as part of this Census application process. Survey respondent work information is not collected.

Version Number: 01-2017

a. Fingerprints ³	x	d. Photographs ⁴	x	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
Other distinguishing features/biometrics (specify): N/A					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	x
b. IP Address	x	d. Queries Run	x	f. Contents of Files	
g. Other system administration/audit data (specify): System administration/Audit data is captured by all CEN08 major applications and general support systems for auditing purposes.					
Other Information (specify)					

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	x	Hard Copy: Mail/Fax	x	Online	x
Telephone	x	Email	x		
Other (specify): N/A					

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies ⁵	x
State, Local, Tribal		Foreign			
Other (specify): N/A					

Non-government Sources					
Public Organizations		Private Sector	x	Commercial Data Brokers	x
Third Party Website or Application			x		
Other (specify): N/A					

2.3 Describe how the accuracy of the information in the system is ensured.

CEN08 Decennial major applications and general support systems uses a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (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 data validation controls to ensure accuracy of information.

³ Explanation for the need to collect, maintain, or disseminate Fingerprints: Fingerprints are only captured 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.

⁴ Explanation for the need to collect, maintain, or disseminate Photographs: 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.

⁵ Selectee fingerprints are processed and submitted to the FBI in support of conducting background investigations for temporary hires and contractors. Survey respondent fingerprints are not collected and no survey respondent data is submitted to the FBI.

Version Number: 01-2017

Selectee information is verified for accuracy when individuals schedule their fingerprints by verification against other forms of identification. Further, the FBI may conduct employment background checks of potential new hires to determine suitability for federal hire.

2.4 Is the information covered by the Paperwork Reduction Act?

x	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Number 0607-1006
	No, the information is not covered by the Paperwork Reduction Act.

2.5 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 ⁶	x
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

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

⁶ Fingerprints are only captured 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.

Version Number: 01-2017

For a Computer Matching Program		For administering human resources programs ⁷	x
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).

The PII collected, maintained, and/or disseminated by the CEN08 Decennial major applications is in reference to members of the public. Data collection is used to produce national statistical information.

The PII collected, maintained, and/or disseminated by Third Party Fingerprinting is in reference to temporary hires and contractors. 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.

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

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

The PII collected, maintained, and/or disseminated by the 2020 Print Vendor is in reference to members of the public. Name and address information is needed to print surveys on physical paper and address envelopes for delivery to survey recipients.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

⁷ Fingerprints are only captured 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 captured and no survey respondent data is submitted to the FBI.

CEN08 Decennial major applications and general support systems adhere to the Information Technology Security Program Policy as it relates to handling, retaining, and disposing collected information. Census Bureau information technology systems employ a multitude of layered security controls to protect 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 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.

Major Applications - Information will be retained for the duration of the Census operations and then disposed of following NIST sanitation guidance.

Third Party Fingerprinting - Fingerprints are retained for 120 days and then disposed of following NIST sanitation guidance. .

R&A- Information will be retained for the duration of the Census operations and then disposed of following NIST sanitation guidance.

DPACS Badging – Information will be retained for the duration of the Census operations and then disposed of following NIST sanitation guidance.

2020 Print Vendor – Information will be retained until contract obligations have been met and then disposed of following NIST sanitation guidance.

All individuals that handle PII are required to complete annual Data Stewardship Awareness training.

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	x	
DOC bureaus			
Federal agencies		x ⁸	
State, local, tribal gov't agencies			
Public			
Private sector		x ⁹	
Foreign governments			

⁸ Personnel PII may be shared with other federal agencies as part of the hiring practice.

⁹ Personnel PII may be shared with private organizations as part of the hiring practice.

Version Number: 01-2017

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	<p>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:</p> <p>Major Applications – Shares information internally within the Census Bureau with 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.</p> <p>General Support Systems: Third Party Fingerprinting – Shares personnel information internally within the Census Bureau with CHEC21 and DPACS Badging as part of the hiring practice.</p> <p>R&A – Shares information internally within the Census Bureau with DAPPS CEN21.</p> <p>DPACS Badging – Shares personnel information internally within Census Bureau DAPPS CEN21 and Third Party Fingerprinting as part of the hiring practice.</p> <p>2020 Print Vendor – No information sharing is conducted by the 2020 Print Vendor.</p> <p>CEN08 Decennial major applications and general support systems uses a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (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 Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.</p>
	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): N/A			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or

Version Number: 01-2017

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 . In addition, a Privacy Act statement is also provided to applicants during the onboarding process.	
	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: Employment with the U.S. Census Bureau is voluntary.
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: According to Title 13, Section 221 of the United States Code ("Census, Refusal or neglect to answer questions; false answers"), persons who fail or refuse to respond to the mail-back census form, or refuse to respond to a follow-up Census Bureau taker can be fined up to \$100. Persons who knowingly provide false information to the Census Bureau can be fined up to \$500. For Census Bureau employees consent to particular uses of PII is a requirement for employment.

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

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Employment with the U.S. Census Bureau is voluntary. Temporary hires and contractors have to consent to the U.S. Census Bureau uses of their PII.
x	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For records covered by SORN Census-5, Decennial Census Programs, there are no access and consent requirements since the data is collected for statistical purposes only. However, PII is protected pursuant to Title 13. For Census Bureau employees consent to particular uses of PII is a requirement for employment.

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: Selectee information is verified for accuracy when individuals schedule their fingerprints.
x	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For records covered by SORN Census-5, Decennial Census Programs, there is no opportunity to review/update data unless the Census Bureau contacts the respondent for an update on their information. For Census Employees, employees have access to PII via the

		of the CEN08 IT system.
--	--	-------------------------

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 within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition to IT system processes that handle PII, all manual extractions for PII 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): <u>July 25, 2018</u> <input type="checkbox"/> 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 (POA&M).
x	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
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.
x	Other (specify): Section 9 of Title 13 requires that the Census Bureau to maintain the confidentiality of the information it collects from decennial census respondents. In addition, it also mandates that the Census Bureau may use such information it collects for statistical purposes, and the information cannot be used to a respondent's detriment. The Census Bureau cannot publish data that identifies a particular individual or establishment, because of Title 13. The Census Bureau leverages its Title 13 authority and obligations in coordination with other federal statutes and mandates for privacy, data security, transparency, and accountability, including the Privacy Act, the E-Government Act of 2002, FISMA, and the Paperwork Reduction Act as well as federal standards and guidance promulgated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Census Bureau information technology systems employ a multitude of layered security controls to protect 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 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 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.”

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> COMMERCE/CENSUS-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/DEPT-13, Investigative & Security Records- http://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-13.html COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html OPM SORN GOVT-5 Recruiting, Examining and Placement Records- https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-5-recruiting-examining-and-placement-records.pdf
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

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.)*

Version Number: 01-2017

x	There is an approved record control schedule. Provide the name of the record control schedule: NI-29-05-01, NI-29-10-5, GRS 3.1, GRS 5.6 item 181
	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	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify):			

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

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. (The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
x	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	PII collected can be directly and indirectly used to identify individuals.
x	Quantity of PII	The collection is for the decennial census, therefore, a severe or substantial number of individuals would be affected if there was loss, theft or compromise of the data. This could affect decennial 2020 Census response rates and have a long term effect on the Nation’s population count. Severe collective harm to the USCB’s reputation, or cost to the USCB in addressing a breach.
x	Data Field Sensitivity	The PII, 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.
x	Context of Use	Disclosure of PII in this IT system or the PII itself may result in severe harm to the individual or organization.
x	Obligation to Protect Confidentiality	PII collected is required to be protected in accordance with 5, U.S.C (552a) and 13, U.S.C, section 9.

x	Access to and Location of PII	<p>The PII 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 regional offices and survey program offices, etc. Access is 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.</p> <p>PII is also located on U.S. Census Bureau authorized vendor systems. Access is limited to those with a need-to-know for authorized U.S. Census Bureau contractors and employees.</p>
	Other:	Provide explanation: N/A

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The collection of PII is required for the 2020 Census, therefore, a severe or substantial number of individuals would be affected if there was loss, theft or compromise of the data. This could affect 2020 Census response rates and have a long term effect on the Nation’s population count, negatively impact appropriations of Federal tax dollars and apportionment of representation in Congress, and jeopardize the reputation of the Census Bureau.

A third party vendor is capturing selectee fingerprint data and PII on behalf of the U.S Census Bureau. The third party vendor is mandated to only utilize authorized systems and FedRAMP solutions. 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.

Census Bureau information technology systems employ a multitude of layered security controls to protect 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 PII has a current authority to operate (ATO) and goes through

Version Number: 01-2017

continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well and requires all individuals to complete annual awareness training.

12.2 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.

12.3 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.