Version Number: 01-2015

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

Privacy Impact Assessment
for the
CEN35 EAD Windows Applications System

Reviewed by: Byron Crenshaw, 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

for Dr. Catrina D. Purvis 07/18/2019

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/EAD Windows Applications System

Unique Project Identifier: 006-00040070

Introduction: System Description

Provide a description of the system that addresses the following elements:.

The CEN35 Applications IT system is hosted at Census Bureau facilities and comprised of three types of applications:

1. The majority of the applications provide support for census and survey data collection, processing, and the dissemination of data.

    a. Data collection through Census Bureau funded censuses and surveys is done for state and local governments, libraries, prisons and other institutions considered public entities[1]. In addition to Census Bureau funded surveys, data collection is done on a reimbursable basis for other sponsors such as the Department of Justice, the National Center for Education Statistics, The Institute of Museums of Museums and Library Services, the Office of Management and Budget, the Department of Education, and the National Science Foundation. (Note: Some data collection is provided by CEN15, Centurion. Centurion is the Census Bureau enterprise solution for the on-line collection of survey or census responses.)

    b. Data processing is done on information collected by CEN35 applications as well as data collected by CEN15: Centurion. The extent of data processing is dependent on the requirements of the individual project.

    c. Data dissemination is done in a variety of ways depending upon the owner of the data and the confidentiality of the data. All data owned by entities external to the Census Bureau is disseminated consistent with the directives of the data owner. Information that is classified as publicly accessible can be posted to public facing internet sites. Information that requires some level of confidentiality has access restricted through identification and authentication functionality.

2. One application included in CEN35 tracks the interview process for prospective Census Bureau employees. This application contains information that is provided as a part of applying for employment, interview scheduling, and notes associated with the interview process for a candidate.

[1] Public entities for this document are federal, state, and local governments; government funded entities; and not-for-profits. Some entities included in this PIA, such as prisons and correctional facilities, may be privately owned. For the sake of simplicity, all of these entities will be referred to as "public entities".

3. One application included in CEN35 is used for Customer/Respondent support; it includes only that information that is provided by respondents who contact the Economics Division with questions about the survey or census to which they are responding.

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

The Typical Transactions are dependent upon the type of application:

1. Census and Survey data
    a. Data Collection: The typical transaction for applications that perform data collection is for a respondent to enter information for the reporting entity into the application's data entry pages.
    b. Data Processing: The typical transaction for data processing is for clerks and/or analysts to review the information and make updates or add information as required.
    c. Data Dissemination: The typical transaction for information dissemination is for a user to view and/or download files to which they have access. Depending upon the type of data, login may be required before the user has access to data.

2. The typical transaction for the interview tracking application is for an approved user to enter information about the interview process for prospective Census Bureau employees.

3. The typical transaction for the respondent support application is for a user to enter information specific to the person who has contacted the Economic Directorate (typically by telephone) to both document their question and identify which survey or census the question is being asked about.

(b) any information sharing conducted by the system

There are three types of information in CEN35 that are shared:

- publicly accessible content that contains no PII/BII
- publicly accessible content that contains PII/BII but is considered 'public' data. For example, government specific data is considered BII, but information about a state government is considered public content or how much a library spent on books in a given year
- access controlled information that includes PII/BII. The access is restricted, through log on functionality, to those with a work related need to have access to the data.

Through CEN35 applications, information is shared in four ways:

- information (publicly accessible content only) is available through public internet sites

- information (publicly accessible content only) is available as 'bulk transfers'
- information is available to external users who have log on credentials
- information is available to internal Census users who have log on credentials

The CEN35 applications do not interconnect with any systems external to CEN35 for information sharing.

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

The legal authority to collect data include:

- 13 U.S.C. Chapter 1, Sections 6 and 8b
- 13 U.S.C. Chapter 5, Sections 131, 132, 161, and 182
- OMB Circular A 133
- OPM GOVT-5: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.
- COMMERCE DEPT 18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

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

The Federal Information Processing Standard (FIPS) 199 category for CEN35 is "moderate".

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.

____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system without changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

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

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age		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): Items i, j, k, l, and p are only maintained within the Interview tracking application.					

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

Distinguishing Features/Biometrics (DFB): Not Applicable					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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

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):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify):					

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

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD):			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Statistical purposes for census and survey data			

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 data is used in very different ways based on the type of application that is associated with it:

1. Census and Survey data shown in Section 2.1 ,
    a. Identifying Numbers (IN): Employer ID
    b. General Personal Data (GPD): Name
    c. Work-Related Data (WRD): Address, Telephone Number, and Email Address.

    This information is collected as a part of identifying the respondent to a census or survey interview. Usage: This information is occasionally used to contact the respondent for additional information or clarification. This information is not disseminated unless the entire response is considered 'public content'. The respondent/person that the information in 2.1 is about is an employee or representative of a public entity.

    The following information is collected as a part of a prison survey:
    d. General Personal Data (GPD): Gender
    e. General Personal Data (GPD): Race/Ethnicity
    f. General Personal Data (GPD): Date of Birth

    This information is collected about prison employees and/or inmates for statistical purposes and is never disseminated at an individual level. Name is not collected and the Census Bureau lacks the information to tie the collected information to an individual. In addition, the Census Bureau only uses this information to generate statistical analyses and does not release the original information.

2. Interview Tracking data includes Section 2.1,
    a. General Personal Data (GPD): Name, Home Address, Telephone Number, Email Address, Education, and Military Service
    b. Work-Related Data (WRD): Occupation, Job Title, Business Address, Salary, and Work History

    This information is collected/maintained when a person submits a resume and/or job application for a job opportunity. Usage: This information is used as a part of the interview process and is never disseminated to the public. The PII in Section 2.1 is for a job applicant who may be a federal employee, a federal contractor, or member of the public.

3. Respondent Support data may include Section 2.1
    a. Identifying Numbers (IN): Employer ID, Employee ID, and/or File/Case ID
    b. General Personal Data (GPD): Name
    c. Work-Related Data (WRD): Address, Telephone Number, and/or Email Address

   This information is collected/maintained when someone contacts the Census Bureau (Economic Programs Directorate) about a census or survey that they are providing the responses for. Usage: The information is collected/maintained with the sole intent of identifying the census or survey that the person is asking about and providing answers to the person's questions. The PII in Section 2.1 is for a person who is a federal employee, federal contractor, or member of the public.

4. All data types in Section 2.1 include System Administration/Audit Data (SAAD): User ID, IP Address, and Date/Time of Access.
   This information is required as a part of the Census Bureau IT Security Program Policy that is based on NIST SP 800-53. Usage: This information is used as a part of the application monitoring (see NIST SP 800-53 for more information on the use of audit logs). Audit logs are generated for the user of the application who can be a federal employee, a federal contractor, or a member of the public.

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	X
DOC bureaus		X	X
Federal agencies		X	X
State, local, tribal gov't agencies		X	X
Public		X	X
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: CEN35 receives information from CEN15: Centurion, which is an Enterprise data collection service as well as some data from CEN03 Economic Census and Surveys and Special Processing CEN35 uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X	Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a privacy policy. The privacy policy can be found at: http://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the application for employment
	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: Prospective employees provide PII when they apply for employment. Some surveys are voluntary. Respondents (people who represent the public sector) have the opportunity to decline some questions.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Some surveys are mandatory; therefore respondents must answer the questions. The data collected is associated with public sector information related to the individual's public sector employment (i.e. name and work contact information only)

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: Prospective employees consent to particular uses of their PII when they apply for employment. Some surveys are voluntary. Respondents have the opportunity to consent to particular uses of their PII.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Some surveys are mandatory therefore, individuals do not have the opportunity to consent to particular uses of their PII. The data collected associated with the individual's public sector employment (i.e. name and work contact information) is mandatory; therefore, individuals do not have the opportunity to consent to particular uses of their PII.

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: Respondent information may be updated through the applicable data collection application.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Applicants do not have the opportunity to review/update PII after it has been submitted unless they gave been hired by the Census Bureau.

Section 8: Administrative and Technological Controls

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

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control *AU-03, Content of Audit records*.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ____7/10/2019_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a DLP solution as well.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: • Commerce/Census – 4, Economic Survey Collection: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html • OPM/GOV-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 • COMMERCE DEPT 18- Employees Personnel Files Not Covered by Notices of Other Agencies: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NC1-29-80-15 GRS 3.1 GRS 3.2 GRS 4.2
	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 Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
X	Quantity of PII	Provide explanation: The collection is for Census Bureau Censuses and surveys, therefore, a serious or substantial number of individuals would be affected if there was loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII, 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	Provide explanation: Disclosure of the act of collecting and using the PII/BII in this IT system or the PII/BII itself may result in serious harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with 13 U.S.C. section 9 or in accordance with 13 U.S.C. section 9b for data associated with Census and Surveys of Governments.
X	Access to and Location of PII	Provide explanation: PII/BII is located on computers and other devices on a network controlled by the Census Bureau. Access limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals (e.g., of sponsoring agencies). Access only allowed by organization-owned equipment outside of the physical locations owned by the organization only with a secured connection.
	Other:	

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.