Version Number: 01-2019

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

Privacy Impact Assessment
for the
CEN35 Economic Applications Division
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

Jennifer Goode 02/04/2021

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: 00600040070

Introduction: System Description

The CEN35 Economic Applications Division (EAD) Windows Applications IT system is hosted at Census Bureau facilities and comprised of four main types of applications:

1. 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.)
2. Data processing is done on information collected by CEN35 applications, data collected by CEN15 Centurion, as well as data obtained from other internal Census Bureau sources. The extent of data processing is dependent on the requirements of the individual project.
3. 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.
4. Analysis/Research - Data Analysis is performed, for approved projects only, to create the results of data analysis which includes, but is not limited to, data products.

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

CEN35 EAD Windows Applications System is a general support system.

(b) System location

CEN35 EAD Windows Applications System servers are physically located in the Bowie Computer Center.

[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".

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

CEN35 EAD Windows Applications System interconnects with the following systems:

- CEN01: Data Communications – provides telecommunications, network infrastructure, and support
- CEN03: Economic Census and Surveys and Special Processing – provides Oracle databases and support
- CEN16: Network Services – provides server and operating systems and support
- CEN17: Client Services – provides desktop and laptop support
- CEN18: Enterprise Applications – provides enterprise level applications/support (ex. SAS) and MS SQL Server databases and support

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

Based on the information in Section 4: Purpose of the System

- *For administrative matters* and *For administering human resources programs* – one application subcomponent is used to track prospective Census Bureau employees through the interview process. All information specific to the individual is the content of the resume which the individual provided as a part application process.
- *To promote information sharing initiatives* – there are three types of PII/BII that are disseminated (i.e. shared) by CEN35.
    i. Information that falls under Title 13 section 9b which does not require the confidentiality of most Title 13 data. This data is made available through public facing websites and/or file transfers. This data is not considered confidential although it falls under the classification of PII/BII.
    ii. Information that is required to be collected and disseminated by federal law or policy. For example, recipients of $750,000 or more in federal grants or required to report how the funds were spent and that information must be disseminated to the public. This data is made available through public websites and/or file transfers. This data is not considered confidential although it falls under the classification of PII/BII.
    iii. Information that is collected on behalf of a sponsor from a federal agency, internal or external to the Census Bureau. This data is considered Title 13 and/or confidential and is shared only through secure file transfers. It is not disseminated to the public.
- *For employee or customer satisfaction* – this information is collected as a part of feedback from application and/or data users. This information is not disseminated to the public and is used only to improve applications and/or data products.
- *Statistical purposes* – one of the primary purposes for collecting and maintaining PII/BII is for statistical (i.e. analysis and research) purposes.

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

Information retrieval by the user is dependent on the type of application:

a. For data collection applications, respondents access their data through a response identifier which identifies the entity or the person reporting. Application administrators retrieve response data based on the response identifier and retrieve user related information based on the userid.
b. For data processing applications, users/analysts retrieve the data based on identifiers that uniquely identify an entity[2].
c. For data dissemination applications that require user log on, users retrieve the data based on identifiers that uniquely identify the entity.
d. For research/analysis projects, users do not retrieve data based on identifiers that uniquely identify an entity.

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

The exact type of information transmission to and from an application is dependent on the type of application:

a. For data collection applications, data transmission leverages TLS 1.2 on the public facing websites. Databases are initialized internally before making the data collection application available to respondents. Encryption is required on all transmissions.
b. For data processing applications, the databases are initialized by automated processes. All applications are available only inside the firewall and encryption is required on all transmissions.
c. For data dissemination applications, data transmission leverages TLS 1.2 on the public facing websites. Encryption is required on all transmissions.
d. For research/analysis projects, all data are available only inside the firewall and encryption is required on all transmissions.

(g) Any information sharing conducted by the system

For CEN35 information, information sharing within the Census Bureau can occur in three ways:

- Case-by-case basis – all parties have a work related need to have access to information for a documented/approved project
- Bulk Transfer – as a part of a documented/approved project, bulk transfer of information is required. An example of bulk transfer that occurs with CEN35 information is information about respondents, both prior to data collection and after the data has been collected.
- Direct Access – many Census Bureau approved projects require that Census Bureau employees have direct access to information in order to analyze and/or process the

[2] A record may be associated with an individual, business, or government.

information. All employees with this type of access have a work related need to have access to the information and have met all training and requirements.

Information sharing with other federal agencies and state, local, and/or tribal agencies are done in two ways:

- Bulk Transfer – when the information is being transmitted to/from the Census Bureau as a part of a document/approved project
- Direct Access – some employees/users from other federal agencies or state, local, and/or tribal agencies require direct access to information. These employees/users must be participants in a project approved by both agencies and then access the information by use of valid identification and authentication credentials.

Information sharing with the private sector and public is done only with a specific type of PII/BII. The PII/BII that is shared is either classified under Title 13 section 9b and/or is specific to an individual in their role as government employee rather than in their role as private citizen. For example, the person's name, government phone number, and government address can be a part of information sharing. A county government name, phone numbers, and address uniquely identify that government making it Business Identifiable Information, however, this information is available to the public and can be shared. The type of information described here is often referred to as public content. Information that is considered public content is shared in two ways:

- Bulk Transfer – files (typically zip files) that group multiple years of information are available to the public. These files contain only public content as described above.
- Direct Access – through search functionality, users can directly access individual responses to specific surveys. These responses contain only public content as described above.

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

The legal authority for collecting, maintaining, using, and disseminating information 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.

(i) The Federal Information Processing Standards (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):					

____ 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.
__X_ 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).
____ 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).

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify): 1) EIN which is required to uniquely identify some business entities. 2) Has a unique number that replaces the SSN but do not have the SSN itself					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X[3]

[3] The only financial information collected within CEN35 is quarterly earnings

b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X		
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. 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 Describe how the accuracy of the information in the system is ensured.

CEN35 applications use 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. In addition to meeting security requirements, • CEN35 data collection applications allow census/survey respondents to update their submissions for the duration of the data collection cycle or as required by the project sponsor with the maximum being up to 6 years. • Data processing and analysis (ex. Edit checks) allow data that is deemed to be inaccurate to be removed and/or replaced.

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. • Survey of Sexual Victimization, OMB Control Number: 1121-0292, Department of Justice, Bureau of Justice Statistics • Single Audit Questionnaire, OMB Control Number: 0607-0518, Census Bureau (sponsored by OMB) • State and Local Government Finance and Public Employment and Payroll Forms, OMB Control Number: 0607-0585, Census Bureau
	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	
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			
For a Computer Matching Program		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 (i.e. analysis and research) purposes			

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. Statistical research and analysis includes all data types in Identifying Numbers (IN), General Personal Data (GPD) and Work-Related Data (WRD) from Title 13, Title 13 section 9b, and Title 26 data.

    This information is analyzed for research purposes which may results in the creation of data/information productions. The Census Bureau never releases the original PII/BII information.

3.Interview Tracking data included 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.

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.

5.2 Describe any potential threats to privacy, such as insider threat, 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.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII 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 Bureau 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

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

The information in the CEN35 is handled, retained and disposed of in accordance with appropriate federal record schedules.

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[4]	X[4]
Private sector		X[4]	X[4]
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 EAD Windows Applications System interconnects with the following systems: • CEN01: Data Communications – provides telecommunications, network infrastructure, and support • CEN03: Economic Census and Surveys and Special Processing – provides Oracle databases and support • CEN16: Network Services – provides server and operating systems and support

[4] Only information that is considered public content is shared with the Public and/or Private sector. For more detail see Introduction letter g.

	• CEN17: Client Services – provides desktop and laptop support • CEN18: Enterprise Applications – provides enterprise level applications/support (ex. SAS) and MS SQL Server databases and support 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[5]	Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

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

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: For the application that pertains to human resources programs (interviews and resumes), notice is provided on the application.
	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 or can choose to decline, but it may affect their employment.. Some surveys are voluntary. Respondents (people who represent the public sector) have the opportunity to decline some questions.

[5] Only information that federal law and/or policy requires public dissemination is made publicly available

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 have 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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): ___July 6, 2020_____ ☐ 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 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.
X	Contracts with customers establish DOC 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. *(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 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 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X___ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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. *(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, 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.)*

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 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, and does not have to be 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.
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. PII/BII maintained/processed/analyzed which includes FTI must be protected in accordance with with IRS-approved procedures put in place.
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:	Provide explanation:

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 U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII 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 Bureau 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

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

Although the enterprise level controls and protections have already been stated, CEN35 meets the requirements that are specific to the applications and projects within CEN35. CEN35 ongoing adherence to security requirements is measured during information system continuous monitoring conducted by OIS. In addition, data collected by CEN35 applications is limited to that data required for the successful completion of the specific project.

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.