Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
U.S. Census Bureau
Office of the Chief Information Officer (OCIO) Applications Development and Services Division (ADSD)
Commerce Business Systems (CBS)

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

TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2024.10.11 13:37:54 -04'00' for Charles Cutshall 8/28/2024

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/ OCIO ADSD Commerce Business Systems (CBS)

Unique Project Identifier: 006-000401400

Introduction: System Description

Provide a brief description of the information system.

Office of the Chief Information Officer (OCIO) Applications Development and Services Division (ADSD) Commerce Business Systems (CBS) (known as CBS going forth) is the financial system of record for the Census Bureau. The OCIO CBS is a major application that provides financial management and accounting capabilities for Budget/Funds Management, Accounts Payable, Accounts Receivable, Reimbursable Agreements, Cost Accumulation, General Ledger, and Financial Reporting. CBS consists of the Core Financial Systems (CFS) computer programs developed by the DOC and Administrative IT systems (called Feeders) developed by Census. CBS collects SSN and other identifying information for required administrative purposes and records management.

CBS is made up of Department of Commerce (DOC) developed programing and programing specific to Census Bureau needs. and includes core financial code developed by the Department as well as Census specific applications developed and managed by Census known as "feeder systems". The CFS program is a central component of CBS and provides the financial management and accounting capabilities to support Census Bureau financial operations.

The Census developed portions of CBS are tested, supported and managed by Census ADSD, while CFS system testing and software development is performed by the DOC CBS Support Center (CSC) with additional operational testing and verification by Census ADSD and Census Finance Division within the Census environment.

Address the following elements:

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

The OCIO CBS is a major application that provides financial management and accounting capabilities for Budget/Funds Management, Accounts Payable, Accounts Receivable, Reimbursable Agreements, Cost Accumulation, General Ledger, and Financial Reporting.

(b) System location

CBS is hosted at the U.S. Census Bureau Computer Center.

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

CBS interconnects with the following internal Census Bureau IT systems to leverage enterprise services: Office of the Chief Information Officer (OCIO) Telecommunications Office (TCO) Data Communications, Office of the Chief Information Officer (OCIO) Computer Services Division (CSvD) Operating System (OS) Services. CBS inherits security controls provided by the Enterprise Common Control Providers (ECCP).

OCIO CBS also interconnects with Office of the Chief Information Officer (OCIO) Field, Associate Director for Field Operations (ADFO) National Processing Center (NPC), Office of the Chief Information Officer (OCIO) Client Support Division (CSD) Client Services, Office of the Chief Information Officer (OCIO) Enterprise Applications, Office of the Chief Financial Officer (OCFO) Systems Data Analysis and Business Solutions Division, Office of the Chief Information Officer (OCIO) Human Resources Applications, and Office of the Chief Information Officer (OCIO) Application Development & Services Division (ADSD) COTS Integration Branch (CIB) Administrative Systems Volume II to share information.

OCIO CBS has interconnections with DOC-wide systems such as CSTARS (Acquisitions System for DOC), Financial Management Service (FMS)/Bureau of the Public Debt, Commerce Learning Center (CLC) and with government-wide systems such as E2 – Government Travel Systems and SmartPay3 (credit card systems at Citibank).

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

The purpose of CBS is for administrative matters. CBS is a major application that provides financial management and accounting capabilities for Budget/Funds Management, Accounts Payable, Accounts Receivable, Reimbursable Agreements, Cost Accumulation, General Ledger, and Financial Reporting.

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

The users utilize the CBS menu system, through a web browser, to access the pieces of the application they are authorized to access. The application pulls data from the Oracle databases and displays it to the users.

Records are retrieved by personal identifiers.

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

Transmitted information between the users and the CBS application is encrypted using HTTPS. There is no public access to CBS.

(g) Any information sharing

CBS shares administrative information with the following internal Census systems:

- Office of the Chief Information Officer (OCIO) Field
- Associate Director for Field Operations (ADFO) National Processing Center (NPC)
- Office of the Chief Financial Officer (OCFO) Systems Data Analysis and Business Solutions Division)
- Office of the Chief Information Officer (OCIO) Human Resources Applications
- Office of the Chief Information Officer (OCIO) Client Support Division (CSD) Client Support Division
- Office of the Chief Information Officer (OCIO) Enterprise Applications
- Office of the Chief Information Officer (OCIO) Application Development & Services Division (ADSD) COTS Integration Branch (CIB) Administrative Systems Volume II.

CBS shares administrative information with the following External systems:

- Department of Commerce - accounting, payment, and PII data
- Financial Management Service (FMS)/Bureau of the Public Debt - Treasury Payment Services
- GSA ETS2 Travel Shared Services – Travel management, payments, and PII data for travel
- GSA SmartPay3 – Credit Card Systems – credit card transactions
- Department of Commerce – Commerce Learning Center – training and PII data

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

28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711, 31 U.S.C. 66(a), 31 U.S.C. 3321 and 40 U.S.C. 486(c), 5 U.S.C. 301

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

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

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.

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*	X	f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Financial transactions and data exchanged with payroll systems are linked to Social Security Number.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name		i. Place of Birth	X	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		l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education	X	t. Mother's Maiden Name	X
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	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. 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		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

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

Other (specify):

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

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

Access to CBS is restricted to those uses with an approved need to the system. Access is role based and users receive access to only those pieces of CBS that they are authorized to use. Oracle database systems maintain audit information about access to the system. The applications have error correction programming to ensure accuracy of data entered.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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	
For administrative matters	X	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):			

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 statements below cover all personnel data within CBS including the information for Census Employees, Census Contractors including Foreign Nationals, and Special Sworn individuals. No personal data regarding the general public is in CBS.

For administrative matters:

a. Social security number (SSN) and/or taxpayer identification number (TIN) identify an individual and "sole proprietor" business where the SSN is used as the identifier or the TIN, whichever is appropriate. Agencies are required to collect TINs [Debt Collection Improvement Act, 31 U.S.C. 7701(c)] and to include the TIN in vouchers submitted for payment [31 U.S.C. 3325 (d)].

b. Name, address and contact information are required to identify and to contact an individual or business. This identifying information is also part of the criteria to identify a vendor to determine eligibility for registration in the General Services Administration (GSA) managed government-wide System for Award Management (SAM.GOV), which replaced the prior Central Contractor Registration (CCR) system.

- Identifying information is needed to identify individuals who require access to secure application code content on the CBS Support Center (CSC) Portal as part of the user account registration process.
- Identifying information is needed to identify individuals who require access to applications as part of the user account registration process.
- Identifying information is used to track transactions and activity performed using the applications.

c. Date and place of birth and mother's maiden name validates the identity of an individual.

d. Bank routing number and individual bank account or electronic funds transfer (EFT) number identify the individual or business and process financial transactions, such as payments.

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 personnel with access to CBS must complete the Mandatory Data stewardship and IT Security Awareness trainings, Title 26 Awareness Training, and No Fear Act Training.

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 and a security operations center to monitor all Census IT system on a 24/7/365 basis.

The information in the CBS 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	X
Federal agencies	X	X	
State, local, tribal gov't agencies			

Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: CBS interconnects with the following internal Census Bureau IT systems to leverage enterprise services: Office of the Chief Information Officer (OCIO) Telecommunications Office (TCO) Data Communications, Office of the Chief Information Officer (OCIO) Computer Services Division (CSvD) Operating System (OS) Services. CBS inherits security controls provided by the Enterprise Common Control Providers (ECCP). OCIO CBS also interconnects with OCIO Field, ADFO NPC, OCIO CSD Client Services, OCIO Enterprise Applications, OCFO Systems Data Analysis and Business Solutions Division, OCIO Human Resources Applications, and OCIO ADSD COTS CIB Administrative Systems Volume II to share information. OCIO CBS has interconnections with DOC-wide systems such as CSTARS (Acquisitions System for DOC), Financial Management Service (FMS)/Bureau of the Public Debt, Commerce Learning Center (CLC) and with government-wide systems such as E2 – Government Travel Systems and SmartPay3 (credit card systems at Citibank). CBS receives information from OCFO Systems Data Analysis and Business Solutions Division, OCIO Human Resources Division, and OCIO ADSD COTS CIB Administrative Systems Volume II. CBS 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 facilities that house Information Technology systems. Census 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.

6.4 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):			

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: https://www.census.gov/about/policies/privacy/privacy-policy.html	
	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.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: CBS does not obtain the information from the individual; HR provides the information.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The information is payroll data. Per 5 U.S.C. 301 a department head may prescribe the regulations for the government of his department including the conduct of its employees and performance of its business, records, & property & individuals do not have opportunity to consent to the uses of the PII that are collected for the purposes stated by the applicable SORNs.

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: Individuals are not able to review/update their PII via CBS but can do so via a Human Resources application or via a Privacy Act Request as per the Privacy Act and as identified in applicable SORN.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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): ____ 7/18/2023 _____ ☐ 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.

	Contracts with customers establish DOC ownership rights over data including PII/BII.
	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 card
- 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 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. Census 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/DEPT-2, Accounts Receivable; https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-2.html COMMERCE/DEPT-17, Records of Cash Receipts; https://www.osec.doc.gov/opog/PrivacyAct/sorns/dept-17.html COMMERCE/DEPT-22, Small Purchase Records; https://osec.doc.gov/opog/privacyact/SORNs/DEPT-22.html COMMERCE/DEPT-25, Access Control and Identity Management System; https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-dept-25
	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: GRS 1.1 GRS 1.1 #10
	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		Overwriting	
Degaussing		Deleting	
Other (specify): OCIO ADSD Enterprise Applications data base administrators delete data using normal methods of deleting from the system during decommission. When servers are decommissioned, OCIO CSvD Network Services standard procedures are used to sanitize data and/or shred as required by Census procedures.			

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.
	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 level. *(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 all U.S. Census Bureau's employees and contractors, therefore, a 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 and using the PII in this IT system or the PII/BII itself may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII in this IT system is collected under the authority of Title 5.
X	Access to and Location of PII	Provide explanation: 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 geographic program area, regional offices, and survey program offices, etc. Access is only 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.
	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.)

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know.

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.

Points of Contact and Signatures