Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
OCIO ADSD CIB Administrative Systems Vol. II

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

BYRON CRENSHAW Digitally signed by BYRON CRENSHAW
Date: 2022.03.17 12:11:46 -04'00'

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/CIB Administrative Systems Vol. II

Unique Project Identifier: 006-000403600

Introduction: System Description

Provide a brief description of the information system.

The name of this system is the Office of the Chief Information Officer (OCIO) Applications Development & Services Division (ADSD) Administrative Systems Vol. II. The system encompasses a wide variety of Administrative Business Solutions within the Census Bureau. Administrative Systems Vol. II applications are used throughout the U.S. Census Bureau to aid in accomplishing its mission in an efficient manner.

These applications provide products and services that ensure a productive and safe work environment. Examples of these systems can be found in section a.

Address the following elements:

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

Administrative Systems Vol. II includes the following applications or components:

- CENdocS (Census Document System) allows for the creation of standard Forms (blank form templates that collect administrative and survey information) and publications. The application also allows Census employees to request graphics and printing services.
- Records Control Database Application which tracks the location of historical & physical records. Expected to be migrated to the Census AWS Cloud using a new Commercial Off the Shelf (COTS) application during FY2022.
- Conference Reservation System (Event Management System (EMS)) professional application is used to manage reservations for the first-floor conference rooms, training rooms, and the auditorium. Access is available to all census employees using the web interface. Expected to be migrated to a Software as a Service (SaaS) COTS at the vendors environment with kiosks, panels, & desktop devices, and will manage all locations in the building during FY2022.
- WorldShare Management System (WMS) Online Computer Library Center (OCLC) [or Ohio College Library Center] Software as a Service (SaaS): WorldShare gives people the ability to view library collections from anywhere in the world. The library staff is the primary user of the Library Management System for checking in and checking out books.

- Environmental Monitoring System (Avtech) is a software/hardware solution to monitor the temperature/ humidity in the HQ Data Centers.
- Enterprise Mail Metering System (Connect+, SendSuite Live) is a collection of mail metering stations located at Census headquarters, the 6 regional offices, and the National Processing Center that are used to place postage on outgoing United States Postal Service (USPS) mail pieces or parcels. The transactions are recorded and later imported into the CBS Postal System. The SendSuite Live on-prem COTS Application is expected to be migrated to SaaS COTS at the vendors environment Send Pro 360 by PitneyBowes during FY2022.
- Correspondence Oversight & Tracking System (CTS) [Entellitrak by Tyler Technologies] is a valuable tool used to route and manage permanent record correspondence between the Director's office and Program Areas within the Census Bureau.

(b) System location

Most of the Administrative Systems Vol. II applications are hosted at Census Bureau Headquarters. The ones that are not, are listed below.

WMS OCLC SaaS's headquarter is in Dublin, Ohio.

Records Control Database Application will be located in the Census Amazon Web Services (AWS) Cloud is located in the AWS GovCloud. AWS headquarters is located in Seattle, Washington.

FM:Systems SaaS application are logically located in AWS US-East-1and AWS US-West-1. The AWS Headquarters is located in Seattle, Washington.

Connect+: The hardware will remain on-prem at the Census Bureau. The SaaS portion will be managed by PitneyBowes whose headquarters is located in Stamford, Connecticut.

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

Administrative Systems Vol. II has an established interconnection with OCIO Commerce Business Systems (CBS) which provides some of the Personally Identifiable Information needed for eligibility to services covered by Administrative Systems Vol. II. It also interconnects with OCIO Data Communications, OCIO Network Services, and OCIO Enterprise Applications for authentication/infrastructure purposes.

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

Administrative Systems Vol. II applications are used throughout the U.S. Census Bureau in accomplishing its mission in an efficient manner. The program areas' web interface tools provide timely, relevant, high-quality products and services.

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

Administrative Systems Vol. II information can be retrieved by an identifier such as name or employee identification. Information contained in the systems are available to authorized U.S. Census Bureau federal employees and contractors.

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

Information is transmitted between Administrative Systems Vol II. and Census Bureau enterprise systems. Components use enterprise supported SQL Server and Oracle databases. Administrative Systems Vol. II also uses enterprise support Lightweight Directory Access Protocol (LDAP) services for user authentication, including Single Sign On. These connections are all encrypted. Administrative Systems Vol. II also receives software updates from external vendors using the HTTPS encrypted protocol. There's an additional connection with a vendor, Pitney Bowes, where electronic funds are downloaded to our postal meters. This connection is also encrypted as required by the United States Postal Service.

(g) Any information sharing

Administrative Systems Vol. II only shares PII from the Mail Metering System by file import to the CBS Postal System. It also queries OCIO CBS for PII.

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

5 U.S.C. 301; 44 U.S.C. 3101; Executive Order 12107, Executive Order 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

Low

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
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:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			

u. Other general personal data (specify):

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		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	
b. IP Address	X	f. Queries Run	X	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	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
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.

PII collected in Administrative Systems Vol II. is voluntary and therefore dependent on the input of the users.

Administrative Systems Vol II. systems employ a multitude of security controls mandated by the Federal Information Security and Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including National Institute of Standards and Technology (NIST) special publications 800 series. These security controls identified include but are not limited to data validation controls to ensure accuracy of information.

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).

For Administrative Matters:
The PII identified in Section 2.1 of this document is in reference to Federal Employees and Census Sworn Employees. The PII collected by the applications covered by Administrative Systems Vol. II are used to identify users, authorize users, and control to applications.

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 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 PII.

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 Administrative Systems Vol. II is handled, retained and disposed of in accordance with appropriate record schedules.

All Census Bureau buildings have physical security and entry requires a valid form of identification such as the agency issued employee badge.

Applications are accessible via Census Bureau internal network and user access is granted based on least privilege and need to know.

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	
DOC bureaus			

Federal agencies			
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.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	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: Administrative Systems Vol. II connects with and receives data from OCIO CBS. It also interconnects with OCIO Data Communications, OCIO Networks Services, and OCIO Enterprise Applications for authentication/infrastructure purposes. The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following: • Intrusion Detection | Prevention Systems (IDS | IPS) • Firewalls • Mandatory use of HTTP(S) for Census Public facing websites • Use of trusted internet connection (TIC) • Anti-Virus software to protect host/end user systems • Encryption of databases (Data at rest) • HSPD-12 Compliant PIV cards • Access Controls 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 (DLP) solution as well. The DLP is an email scan of unencrypted email messages and attachments to detect inappropriate transport of sensitive information.
	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: http://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: The PII collected by the applications covered by Administrative Systems Vol. II are used to identify users, authorize users, and control to applications. In order to use the system(s) PII/BII is a requirement.

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 PII collected by the applications covered by Administrative Systems Vol. II are used to identify users, authorize users, and control to applications. In order to use the system(s) PII/BII is a requirement.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The Administrative Systems Vol. II receives PII/BII from other Census' IT systems and do not store the PII/BII. Opportunities to review/update PII/BII are made available through the original IT system used to collect and/or store the PII/BII.

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 13, 2021 _____ ☐ 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).*

The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following: • Intrusion Detection | Prevention Systems (IDS | IPS) • Firewalls • Mandatory use of HTTP(S) for Census Public facing websites • Use of trusted internet connection (TIC) • Anti-Virus software to protect host/end user systems • Encryption of databases (Data at rest) • HSPD-12 Compliant PIV cards • Access Controls 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 (DLP) solution as well. The DLP is an email scan of unencrypted email messages and attachments to detect inappropriate transport of sensitive information.

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-18, Employees Personnel files not covered by notices of other agencies: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html COMMERCE/DEPT-19, Mailing List https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-19.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: GRS 3.1, GRS 3.2, Records Schedule NCI-29-84-1
	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	
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.)*

X	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.
	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: Data elements are not directly identifiable alone but may indirectly identify individuals or significantly narrow large datasets.

X	Quantity of PII	Provide explanation: A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, have little relevance outside the context.
X	Context of Use	Provide explanation: Disclosure of PII is unlikely to result in limited harm to the individual or organization such as name, address, and phone numbers of a list of people who subscribe to a general-interest newsletter.
X	Obligation to Protect Confidentiality	Provide explanation: Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.
X	Access to and Location of PII	Provide explanation: Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. PII is not stored or transported off-site by employees or contractors.
	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 threat to privacy is low due to the low sensitivity level of the PII collected under this IT system. Loss of PII data will cause a minimal effect on the individuals affected. Collection of PII data for Administrative Systems Vol. II is important for administering administrative and operational support services.

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.