Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Associate Director for Decennial Census Program (ADDCP)
Geography

Reviewed by: Monique Eleby, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER Date: 2025.08.20 14:01:03 -04'00' 8/20/25

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau ADDCP Geography

Unique Project Identifier: 006-000400900

Introduction: System Description

Provide a brief description of the information system.

ADDCP Geography is a suite of information technology (IT) applications and databases used to support the Geography Division's mission of providing "…high-quality geographic data and products to customers across the Census Bureau; to tribal, federal, state, and local governments; and to the public." These applications and databases include commercial-off-the-shelf, government-off-the-shelf, and in-house-developed technologies with varying architectures and levels of complexity. Information within ADDCP Geography is primarily geographic and address data used for geographic framing for agency surveys and censuses. These data originate from tribal governments, state governments, local governments, other federal agencies, commercial sources, and Census and Survey responses. These data are applied to the Master Address File (MAF)/Topologically Integrated Geographic Encoding and Referencing (TIGER) System known as the "MAF/TIGER System.

The MAF/TIGER System is the U.S. Census Bureau's geospatial inventory of addresses, features, and boundaries covering the fifty states, Washington DC, Puerto Rico and the Island Areas. Data and products from the MAF/TIGER System form the foundation of essential Census Bureau programs by providing the framework for survey design, sample selection, data collection, data tabulation and data dissemination.

The MAF/TIGER System is an overarching system of more than 100 applications and databases that provide the geographic products and services required to conduct Censuses and Surveys. This system also provisions geographic products and applications that support and serve tribal, state, and local government agencies; federal agencies; and the American public.

The Census Bureau relies on data received in a variety of geographic partnership programs, such as the Boundary and Annexation Survey (BAS) and Local Update of Census Addresses (LUCA) programs; address data from partner agencies such as the United States Postal Service (USPS); and parcel data from commercial vendors to enhance and improved the quality of the boundaries, addresses, and geographic information in the MAF/TIGER System. This data is processed through a number of batch and interactive processes with the overarching goal of ensuring that the data in the MAF/TIGER System is complete and accurate.

ADDCP Geography acquires several parcel data datasets from commercial sources and vendors. Parcel vendors aggregate comprehensive parcel data by collecting and standardizing information from a variety of sources, primarily public datasets; these sources include county assessor offices, tax records, zoning maps, and land-use databases. By consolidating and

refining this information, they create accessible, standardized datasets for geospatial analysis. Parcel datasets are used by ADDCP Geography to identify new housing units and to locate housing units. Parcel datasets contain PII upon acquisition, but the PII are not used and are removed from the datasets by the ADDCP Geography. ADDCP Geography downloads the parcel data from a secure file transfer protocol (SFTP) site. The parcel data is transformed into a national Oracle table, minus the PII data, using the Feature Manipulation Engine (FME), which is an automated tool. The results of this processing are sent to MAF address matching.

ADDCP Geography also includes information technology (IT) applications that provide external partners (tribal governments, state governments, and local governments), the ability to provide their contact information to the Census Bureau Geography Division. Contact information provided by the partnering governments is used by the Geography Division to facilitate the administration of Geographic Programs. The three applications are:

The Geographic Program Participant (GPP) application is an internal database system that contains the contact information for external partners who participate in the Census Bureau's Geographic Partnership Programs. The GPP maintains a link between a contact person and their respective geographic entity or organization. The contact data seen in the GPP includes, but is not limited to: Name, Position, Mailing Address, Email Address, and Phone Number. Importantly, and through a direct interface, the GPP provides these data to the Geography Division Partner Portal (GDPP).

The GDPP is the centralized information hub for Geographic Partnership Programs. Within the GDPP, partners have streamlined access to Census Bureau geographic and statistical data, program invitations, historical participation information, and contact information. Additionally, partners can communicate with the Geography Division program areas through a centralized communication system.

ADDCP Geography also includes an information technology (IT) application, the Geographic Update Partnership Software (GUPS), that provides external partners (tribal governments, state governments, and local governments) the ability to update geospatial data, attributes, and addresses for Census Bureau geographic partnership programs. Updates to geospatial data, attributes, and addresses provided by the partnering governments is used by the Geography Division to update the MAF/TIGER System.

Address the following elements:

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

The MAF/TIGER System is a general application support system composed of more than 100 applications and databases that provide the geographic products and services required to conduct Censuses and Surveys.

(b) *System location*

ADDCP Geography applications and databases are hosted and managed within the Census Bureau Computer Center located in Bowie, MD, the Oracle Government Cloud located in Ashburn, Virginia, the Google Cloud Platform located in Ashburn, Virginia, and the AWS GovCloud (US-East/ Columbus, Ohio) and AWS GovCloud (US- West/ Portland, Oregon) Regions located in the Eastern and Northwestern parts of the United States.

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

Within the Census Bureau network, the ADDCP Geography applications interconnect with infrastructure services at the U.S. Census Bureau. This includes Office of the Chief Information Officer (OCIO) Data Communications for authentication/ telecommunication purposes, OCIO Network Services for server/storage, OCIO Client Support Division (CSD) for laptops and workstations and OCIO Enterprise applications for database support.

The ADDCP Geography applications also interconnect with applications in other areas of the Census Bureau applications including:

- Associate Director for Field Operations (ADFO) National Processing Center (NPC)
- Associate Director for Decennial Census Programs (ADDCP),
- Associate Director for Demographic Programs (ADDP),
- Associate Director for Research & Methodology (ADRM) Cloud Research Environment (CRE),
- ADRM Integrated Research Environment
- OCIO Enterprise Data Lake (EDL),
- OCIO Data Ingest and Collection for the Enterprise (DICE),
- ADDCP American Community Survey Office (ACSO), and
- Associate Director for Economic Programs (ADEP)

This extensive list of data exchange interconnections is due to Geography's central role of provisioning address and geospatial data to many Surveys and Programs within the Census Bureau.

The Census Bureau also has a direct connection account with the USPS to receive delivery point address data.

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

Geography receives address and geospatial data from internal Census Bureau systems, the USPS; tribal, state, and local governments; federal agencies; Census Bureau field operations, and commercial sources. These data populate the MAF/TIGER System. Geography receives these data, and these data are used in the tabulations produced by various Census Bureau statistical

programs.

Per the Public Law 103-430 (Census Address List Improvement Act of 1994) amended Census Bureau Title 13 and USPS Title 39, allowing USPS to provide the delivery sequence files to the Census Bureau, which include all delivery point addresses.

Geography obtains parcel data directly from a commercial vendor and the Department of Homeland Security to identify new housing units and to locate housing units. The data include PII such as parcel owner name, owner address, and situs address. The PII (parcel owner information) is not used in Geography's data processing and is removed prior to update of the MAF, via an automated tool. ADDCP Geography downloads the parcel data from a secure file transfer protocol (SFTP) site. The parcel data is transformed into a national Oracle table, minus the PII data using the Feature Manipulation Engine (FME) which is an automated tool. The results of this processing are sent to MAF address matching. While parcel address data is shared within the Bureau, parcel owner information, from parcel address data, is not shared within the bureau. Parcel address data is not shared outside of the Bureau.

Geography provides a data file to the Census Bureau program area that conducts the American Housing Survey (AHS) every two years. This file provides information related to how the latitude and longitude coordinates of the MAF address units in the AHS sample match to parcels in a commercial parcel dataset based on their spatial location and address information.

Geography has received building permits data for Carroll and Frederick Counties from the Maryland Department of Planning as part of the joint statistical agreement and project between the two organizations. The data files contain the name of the person(s) or business to whom the permit was issued as well as the address of the location associated with the permit. These files are used for research purposes only to assess the kind of information contained on building permit records and how such information might be used to detect and manage changes to the inventory and attributes of addresses, residential units, and nonresidential units. This data is not shared within the bureau or outside of the bureau.

As part of its partnership programs, especially the Boundary and Annexation Survey (BAS) and the Local Update of Census Addresses (LUCA) programs, Geography collects the names, governmental emails, governmental addresses, and governmental telephone numbers of governmental personnel. These data are stored in the Geographic Program Participant (GPP) application and Geography Division Partner Portal (GDPP) application databases and will be managed by the participating partners via the GDPP application. Program participants may retrieve PII data stored in the GDPP application by personally identifiable information.

To support conduct of the 2020 Decennial Census Group Quarters (GQ)/ Transitory Location (TL) operations, Geography maintained a repository of GQ contact information, including

contact information not in MAF/TIGER such as GQ contact email. The information in the GQ Production Control System was from MAF/TIGER and collected from sources such as the 2020 Decennial Census GQ Advance Visit operation. This information was also used to communicate with the GQ administrators to arrange visits or other methods of enumeration, and the GQs were not sampled by the contact information. Group Quarters contact person name, title, and telephone number are stored in the MAF/TIGER database. These data were collected from a variety of decennial census in-field and in-office operations, demographic surveys, American Community Survey (ACS) operations, and administrative sources. Group Quarters operations across the Census Bureau depend on the GQ contact information to communicate with the GQ administrators to arrange visits or other methods of enumeration. Group Quarters are not sampled by the GQ contact information.

Geography utilizes its partner portals to provide external governmental partners (tribal governments, state governments, and local governments), the ability to provide their contact information to the Census Bureau Geography Division. Contact information provided by the partnering governments is used by the Geography Division to facilitate the administration of Geographic Programs. Partners can view contact details for the government for which they are associated and are invited to provide suggested updates to their contact information previously provided. The contact information provided includes partner name, mailing address(es), phone number(s), and email addresses.

The Geographic Program Participant (GPP) application is an internal database system that contains the contact information for external partners who participate in the Census Bureau's Geographic Partnership Programs. The GPP maintains a link between a contact person and their respective geographic entity or organization. The contact data seen in the GPP includes, but is not limited to: Name, Position, Mailing Address, Email Address, and Phone Number. Importantly, and through a direct interface, the GPP provides these data to the Geography Division Partner Portal (GDPP).

The GDPP is the centralized information hub for Geographic Partnership Programs. Within the GDPP, partners have streamlined access to Census Bureau geographic and statistical data, program invitations, historical participation information, and contact information. Additionally, partners can communicate with the Geography Division program areas through a centralized communication system.

Geography provides government boundary and address information in the Geographic Update Partnership Software (GUPS) to logged-in external partners (tribal governments, state governments, and local governments); authorized governmental partners can view geospatial data, attributes, and address details for the government for which they are associated. Partners are invited to voluntarily provide suggested updates to their geospatial data, attributes, or address

information previously provided.

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

For most MAF/TIGER applications and databases, retrieval is by geographic and address attributes. Authorized users' interface with the information contained within the MAF/TIGER System applications and databases using authorized web applications and file servers that are protected with a multi-layer security approach.

Within the partner portals, authorized governmental partners can view and retrieve contact details and information for the contacts in the government for which they are associated. Authorized governmental partners can access this data by selecting the name or government they have approved access to view.

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

Information is received from systems within the Census Bureau and other federal agencies via secured electronic data transfer mechanisms. Information is received from the U.S. Postal Service via a secured file transfer protocol (SFTP). In addition to those Federal sources, information is transmitted to and from partner governmental entities and organizations at the tribal, state, and local levels via secured electronic data transfer mechanisms.

Information is also transmitted via annotations on printed listing forms and cartographic maps.

(g) Any information sharing

Title 13 addresses are shared with other Census Bureau programs with a work-related need-to-know and partner governmental entities and organizations at the tribal, State, and local levels[1].

The GPP shares internally to Geography with the GDPP. The GDPP does not share point of contact information with other systems; however, individuals are able to see contact information about other individuals within their own governmental jurisdiction.

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

[1] 2030 Census Local Update of Census Addresses Operation (LUCA) is an opportunity for officials of tribal, state, and local governments to engage with the 2030 Census by reviewing and commenting on the U.S. Census Bureau's address list prior to the 2030 Census. Governments who agree to protect the confidentiality of our address list can receive the addresses for their jurisdiction through the LUCA operation. More information about LUCA can be found here: https://www.census.gov/programs-surveys/decennial-census/decade/2030/planning-management/where/2030-census-luca.html

13 U.S.C. 6(c), 141 and 193
Title 26
National Geospatial Data Act

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

The FIPS 199 security information standard 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.
_X__ 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	X
c. Significant System Management Changes		f. Commercial Sources	X	i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Geography Division did not previously have a PIA since they only collected/processed addresses and geographical attributes. Geography Division now includes partner portals that provide tribal governments, state governments, and local governments the ability to provide their contact information and to update geospatial data, attributes, and addresses for Census Bureau geographic partnership programs to the Census Bureau Geography Division.					

____ 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.

____ 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		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	X	q. Military Service	

d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	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	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	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		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		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	X[2]	Online	X[2]
Telephone	X[2]	Email	X[2]		
Other (specify):					

Government Sources

[2] Partners (Tribal governments, state governments, and local governments) can provide their contact information to the Census Bureau Geography Division via phone, email, mail, and/or online.

Within the Bureau	X[3]	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify): PII information is received through parcel data files that are received from the Department of Homeland Security (DHS).					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	X
Third Party Website or Application			X[4]		
Other (specify): PII information is received through parcel data files that are received from commercial sources and vendors.					

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

In terms of the PII received in the parcel data files, direct identifiers are purged from the data files immediately after receipt so that only geolocation and address information remains.

The PII received from partner governments and organizations is validated for accuracy. Validation checks are performed through manual research including phone calls, emails, and web searches.

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. Boundary and Annexation Survey (BAS): 0607-0151 Redistricting Data Program (RDP): 0607-0988 School District Review Program (SDRP): 0607-0987 Spatial, Address, and Imagery Data (SAID) Program: 0607-1008
	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	

[3] GDPP receives data from another internal Geography application, the GPP
[4] Data may be collected about partners online, from non-governmental websites.

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	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	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For statistical 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).

For Statistical Purposes: Geography receives address and geospatial data from internal Census Bureau systems, the U.S. Postal Service (USPS); tribal, state, and local governments; federal agencies; Census Bureau field operations, and commercial sources. These data populate the MAF/TIGER System. Geography receives these data, and these data are used in the tabulations produced by various Census Bureau statistical programs. Geography obtains parcel data directly from a commercial vendor; the data include parcel owner name, owner address, and situs address. The parcel owner information is not used in Geography's data processing and is removed, via an automated tool, prior to update of the MAF.

For Administrative Matters & Information Sharing: PII is collected about partners, which are currently tribal, state, and local government employees, to maintain the point of contact information.

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

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[5]		
DOC bureaus			
Federal agencies	X[5]		
State, local, tribal gov't agencies	X[5]		X[6]
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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-

[5] Title 13 addresses (just addresses, no identifiable information is included) are only shared with other Census Bureau Programs with a work-related need-to-know, partner governmental entities and organizations at the tribal, State, and local levels.
[6] Within the GDPP, individuals are able to see contact information about other individuals within their own jurisdiction.

	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: Information is received from systems within the Census Bureau and systems at other federal agencies (U.S. Postal Service for example) via secured electronic data transfer mechanisms. In addition to those Federal sources, information is transmitted to and from partner governmental entities and organizations at the tribal, State, and local levels via secured electronic data transfer mechanisms. Within the Census Bureau network, the Geography applications interconnect with infrastructure services at the U.S. Census Bureau. This includes OCIO Data Communications for authentication/ telecommunication purposes, OCIO Network Services for server/storage, OCIO Client Support Division (CSD) for laptops and workstations and OCIO Enterprise applications for database support. ADDCP Geography applications also interconnect with applications in other areas of the Census Bureau applications including: • Associate Director for Field Operations (ADFO) National Processing Center (NPC) • Associate Director for Decennial Census Programs (ADDCP), • Associate Director for Demographic Programs (ADDP), • Associate Director for Research & Methodology (ADRM) Cloud Research Environment (CRE), • Office of the Chief Information Officer (OCIO) Enterprise Data Lake (EDL), • OCIO Data Ingest and Collection for the Enterprise (DICE), • ADDCP American Community Survey Office (ACSO), • Associate Director for Economic Programs (ADEP), and • Census Bureau initiatives such as Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI) and Frames. This extensive list of data exchange interconnections is due to Geography's central role of provisioning address and geospatial data to many Programs within the Census Bureau. 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.
	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): Authorized governmental partners can view contact details for the contacts in the government for which they are associated. Partners are invited to provide suggested updates to their contact information previously provided and geospatial data, attributes, and addresses for Census Bureau geographic partnership programs.			

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 Privacy Act Statements are provided to external governmental partners that are inputting their information in the partner portals.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Privacy Act Statements are provided to external governmental partners that are inputting their information in the partner portals. Participation in the GDPP is voluntary.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Parcel data is received from commercial sources. There is no opportunity to decline.

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 Privacy Act Statements are provided to external governmental partners that are inputting their information in the partner portals. Participation in the GDPP is voluntary.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Parcel data is received from commercial sources. There is no opportunity to consent to particular uses.

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 can submit suggested updates to their own contact information via the GDPP.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Parcel data is received from commercial sources. There is no opportunity to review/update.

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): _____June 30, 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.
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) and during transit
• 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 Data Loss Prevention solution and a security operations center to monitor all Census IT system on a 24/7/365 basis.

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-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs: https://www.commerce.gov/node/4958
	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: DAA-0029-2019-0004, Nl-29-05-01, N1-29-10-5, GRS 1.3, GRS 3.1, GRS 5.6 item 181
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing		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: Addresses alone are not identifiable. The partner contact information is publicly available information.
X	Quantity of PII	Provide explanation: While the quantity of addresses is high, addresses alone are not identifiable.

X	Data Field Sensitivity	Provide explanation: PII within the Geography Systems is not sensitive.
X	Context of Use	Provide explanation: Disclosure of PII is unlikely to result in harm to the individual or organization as PII is limited to addresses and publicly available contact information for Census Bureau partners.
X	Obligation to Protect Confidentiality	Provide explanation: The Geographic Support Program collects, maintains, and disseminates data under the authority of Title 13. The Geographic Support Program also processes data, specifically addresses extracted from Federal tax information, under the authority of Title 26. The Geographic Support Program has annual reporting obligations to the Federal Geographic Data Committee (FGDC) that are mandated by the National Geospatial Data Act. The Geographic Support Program is the lead for the Census Bureau's management of the Address (co-lead with the Dept. of Transportation) and Governmental Units and Administrative and Statistical Boundaries data themes. The Census Bureau's geographic boundary data are considered the authoritative source for this information with their designation as National Geospatial Data Assets by the FGDC.
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. Access is allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Data is also located on U.S. Census Bureau authorized vendor systems. Access is limited to those with a need-to-know for authorized U.S. Census Bureau contractors and employees.
	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