Version Number: 01-2020

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

Privacy Impact Assessment
for the
Cloud Services

Reviewed by: Byron Crenshaw, Bureau Chief Privacy Officer

☉ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 09/30/2021

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau, Office of Chief Information Officer: Cloud Services

Unique Project Identifier: N/A

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

Cloud Services is a general support system. The Cloud Services general support system houses cloud-based systems/components utilized by the U.S. Census Bureau. This system can be described as the U.S. Census Bureau's framework for cloud computing. Services/components in Cloud Services spans multiple servers, and the physical environment is typically owned and managed by a third-party vendor at offsite facilities located in the United States. The third-party vendors used are Federal Risk and Authorization Management Program (FedRAMP) authorized Cloud Service Providers (CSPs). These third-party cloud providers are responsible for keeping the data/information available and accessible, and the physical environment protected and running. Cloud services are bought or leased from the cloud provider, which transmits and stores user, organization, and application data.

(b) System location

AWS GovCloud is located in Oregon and Ohio
AWS East-1 is located in Virginia and East-2 is located in Ohio
AWS West-1 is located in California and West-2 is located in Oregon
Microsoft Azure paired regions are located in Iowa and Virginia

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

Cloud Services connects with/receives/maintains data from U.S. Census Bureau's IT systems that are hosted on the Cloud Services' Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

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

Cloud Services is the U.S. Census Bureau's framework for cloud computing. Cloud Services are bought or leased from the FedRAMP authorized cloud provider and utilized by the U.S. Census Bureau to transmit, process and/or store user, organization, and application data. The technology

or components in this system span multiple servers, and the physical environment is typically owned and managed by a third-party vendor at offsite facilities located in the United States. These third-party cloud providers are responsible for keeping the data/information available and accessible, and the physical environment protected and running.

The two current service models within Cloud Services are:

1) Infrastructure as a Service (IaaS) – as defined by the NIST Special Publication 800-145 – the customer is provided processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

   The following IaaS are authorized to operate in Cloud Services:

   a. Amazon Web Services GovCloud U.S. region is a logically isolated AWS Regions located in the states of Oregon and Ohio designed to allow U.S. government agencies and contractors to move more sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. Customer applications are built upon the standard AWS services, and are managed under their corresponding system boundary at the U.S. Census Bureau's Directorate level. Customers are responsible for managing the security controls within their application.

   b. Amazon Web Services East/West located in U.S. East (Northern VA and Ohio) and U.S. West (Northern CA and Oregon) regions are utilized under the IaaS cloud computing model. The Amazon Web Services East/West IaaS enables convenient, on-demand Internet access to a shared pool of configurable Amazon Web Services computing resources such as servers, storage, network infrastructure, applications, and additional services. The U.S. Census Bureau is responsible for providing standard deployment and configuration of the IaaS offerings. Customer applications are built upon the standard AWS services, and are managed under their corresponding system boundary at the U.S. Census Bureau's Directorate level. Customers are responsible for managing the security controls within their application.

2) Platform as a Service (PaaS) – as defined by the NIST Special Publication 800-145 – the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

   The following PaaS is authorized to operate in Cloud Services:

a. Amazon Web Services GovCloud logically isolated regions located in the states of Oregon and Ohio provide Platform as a Service (PaaS) and software tools, needed for application development, to its customers as a service. A PaaS provider hosts the hardware and software on its own infrastructure. As a result, the PaaS frees the customers from having to install in-house hardware and software to develop or run a new application. The U.S. Census Bureau currently offers managed shared web service that makes it easy to set up, operate, and scale databases in the cloud. These services are available for deployment with the AWS GovCloud infrastructure. The U.S. Census Bureau is responsible for providing standard deployment and configuration of the PaaS offerings. Tenant applications leveraging the PaaS offerings are managed under their corresponding system boundary at the U.S. Census Bureau's Directorate level.

b. Amazon Web Services located in U.S. East (Northern VA and Ohio) and U.S. West (Northern CA and Oregon) regions are utilized under the PaaS cloud computing service model. The Amazon Web Services Platform Service Management comprise managed web services that makes it easy to set up and operate services in the cloud. The U.S. Census Bureau creates instances and secure configurations that are uniform across the enterprise. The U.S. Census Bureau is responsible for providing standard deployment and configuration of the PaaS offerings. Customers are responsible for managing the security controls within their application and corresponding system boundary at the U.S. Census Bureau's Directorate level.

Cloud Services stores and maintains Personally Identifiable Information (PII) /Business Identifiable Information (BII) for different program areas at the U.S. Census Bureau. Access to this data is only accessible by Cloud Services on the administrative level. Cloud services IaaS and PaaS do not perform data dissemination however the IT systems hosted on Cloud Services may.

The following FedRAMP cloud-based technology offerings are currently within scope of the U.S. Census Bureau's agile authorization methodology for inclusion into the Cloud Services authorization to operate:

a. Microsoft Azure Commercial Cloud is an open and flexible cloud platform that enables customers to quickly build, test and deploy, and manage their applications, services, and product development across a network of Microsoft managed datacenters within the United States. Microsoft Azure provides a multi-tenant public cloud services platform that offers functionality to support capacities such as Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) under the FedRAMP shared-responsibility cloud computing models.

b. Microsoft Azure Government is a government-community cloud that offers hyper-scale compute, storage, networking, and identity management services, with world-class security. A physically and network-isolated instance of Microsoft Azure, operated by screened U.S. citizens, Azure Government provides standards-compliant IaaS and PaaS under the FedRAMP shared-responsibility cloud computing models.

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

Cloud Services stores and maintains PII/BII for different program areas at the U.S. Census Bureau. Cloud Service's cloud providers do not have access to the encryption keys of U.S. Census Bureau's data so do not have access to the data.

Cloud Services is not a system of records, therefore information is not retrieved at the PaaS and IaaS level by personal identifier.

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

Information is transmitted to and from IaaS and PaaS cloud services only for authorized and lawful government purposes by employing secure communications with layered security controls including, but not limited to the use of validated FIPS 140-2 cryptographic modules and mechanisms to protect PII/BII.

(g) Any information sharing conducted by the system

Applications and software, covered by other U.S. Census Bureau's authorization boundaries, residing on the Cloud Services IaaS and PaaS may share PII/BII. The PII/BII in the Cloud Services is only shared within the U.S. Census Bureau on the fundamental of authorized work-related need-to-know basis. The only documented case for Cloud Services to share PII/BII with another agency via direct access and/or bulk transfer is the transfer of permanent electronic records to the National Archives and Records Administration (NARA) for accessioning purposes per Executive Office Memorandum M-19-21, Transition to Electronic Records.

Each service model provides a means to facilitate the secure transfer/storage/processing of the model's respective data. Encryption at rest and encryption during transport are enforced in the Cloud Services' cloud environments.

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

It has been determined that Cloud Services is not a system of records. As a result, information systems containing PII/BII that are hosted on Cloud Services are governed by the SORN(s) specific to the record types stored within the information system and must be used in accordance with the purpose(s) enumerated in the SORN. The legal authorities for each information system, containing PII/BII hosted on the Cloud Services infrastructure, can be located in its respective SORN.

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

The FIPS 199 security impact category for Cloud Services 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	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): There has been a scope change to Cloud Services with the inclusion of an additional FedRAMP cloud service provider and cloud services to accommodate new hosts that utilize Cloud Services' IaaS and PaaS.					

____ 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 (version 01-2015 or 01-2017).
____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card		m. Medical Record	X
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: SSN could reside in authorized information systems designed and deployed for such purpose within the U.S. Census Bureau's authorized FedRAMP boundary. Individual IT system PIA's will contain SSN justifications and the applicable legal authorities. When SSNs are present in these data they serve as one of several components used in a matching or look-up process to assign an anonymized protected identification key (PIK) to the record.					

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

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
c. Work Address	X	g. Work History	X	k. Procurement/ Contracting Records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
k. 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	X	n. Retina/Iris Scans	
e. Photographs		j. Weight	X	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		f. Contents of Files	X
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		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.

The accuracy of information is ensured by the program areas that hosts their applications on the Cloud Services cloud environment. Cloud Services' cloud environments implement encryption at rest and encryption during transport to maintain the integrity of information on hosted systems. Cloud Services' cloud providers do not have access to the encryption keys of U.S. Census Bureau's data.

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. OMB 0607-0725; 0607-0978; 0607-0971, 0607-0995, 0607-1013
	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 no 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 no 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): To provide infrastructure capabilities to U.S. Census Bureau's information systems for statistical purposes (i.e. Censuses/Surveys).			

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:
Authentication information is received from U.S. Census Bureau's Identity and Access Management capabilities for employees and contractors authentication purposes. This is used to provide access to the computing environments.

The PII collected in Section 2.1 System Administration/Audit Data (SAAD) and maintained by Cloud Services is used for administrative purposes. The PII is collected from federal employees and contractors that use Cloud Services' IaaS and PaaS. User ID's, IP Addresses, Date and Time of Access, are collected for user access and cybersecurity investigative purposes.

Other:
PII/BII received from other systems is maintained on Cloud Services via it's IaaS and PaaS capabilities; data is not disseminated at this level. This data refers to all PII/BII maintained by other U.S. Census Bureau's information systems – including data received from the public, federal employees, contractors, foreign nationals, and visitors.

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's employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

In addition, the U.S. Census Bureau's information 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 U.S. Census Bureau's 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 U.S. Census Bureau's information 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 U.S. 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 U.S. Census Bureau also deploys a Data Loss Prevention solution.

Cloud Services' cloud service providers do not have access to the encryption keys of U.S. Census Bureau's data so do not have access to the data. The information in the Cloud Services system is handled, retained and disposed of in accordance with appropriate 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
DOC bureaus			
Federal agencies[1]	X	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?

X	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.
	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.

[1] The PII/BII in the system is only shared within the U.S. Census Bureau on the fundamental of authorized work-related need-to-know basis. The only documented case for Cloud Services to share PII/BII with another agency via direct access and/or bulk transfer is the transfer of permanent electronic records to the National Archives and Records Administration (NARA) for accessioning purposes per Executive Office Memorandum M-19-21, Transition to Electronic Records.

	Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Cloud Services receives authentication information from U.S. Census Bureau's Identity and Access Management capabilities. Cloud Services also connects with/maintains data from U.S. Census Bureau's IT systems that are hosted on the cloud environment (IaaS and PaaS). The IT system uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at U.S. Census Bureau's facilities that house information systems. The U.S. Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well. An email message archive system connects to the U.S. Census Bureau's email service/mail servers to extract email messages for archival purposes.
	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.)*

	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 at the program area level for collections maintained by other IT systems hosted by Cloud Services	
X	Yes, notice is provided by other means.	Internal Systems Only U.S. Census Bureau Notice and Consent Warning You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all computers connected to this network, and 4) all devices and storage media attached to this network or to a computer on this network.

		You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and for any lawful Government purpose; the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. **Publicly Accessible Systems Only** U.S. Census Bureau Notice and Consent Warning You are accessing a United States Government computer network. Any information you enter into this system is confidential. It may be used by the Census Bureau for statistical purposes and to improve the website. If you want to know more about the use of this system, and how your privacy is protected, visit our online privacy webpage at http://www.census.gov/about/policies/privacy/privacy-policy.html. Use of this system indicates your consent to collection, monitoring, recording, and use of the information that you provide for any lawful government purpose. So that our website remains safe and available for its intended use, network traffic is monitored to identify unauthorized attempts to access, upload, change information, or otherwise cause damage to the web service. Use of the government computer network for unauthorized purposes is a violation of Federal law and can be punished with fines or imprisonment (PUBLIC LAW 99-474). This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy.
	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: PII is pulled from other U.S. Census Bureau's information systems; therefore, there is not an opportunity to decline to provide PII at the Cloud Services system level.

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: PII is pulled from other U.S. Census Bureau's information systems; therefore, there is not an opportunity to consent to particular uses of PII at the Cloud Services system level.

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: PII is pulled from other U.S. Census Bureau's information systems; therefore, there is not an opportunity to review/update PII at the Cloud Services system level.

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 within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition, audit logs are in place and assessed per 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 23, 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).*

U.S. Census Bureau's information 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)
- Encryption of data in transit HTTPS/SSL/TLS
- HSPD-12 Compliant PIV cards
- Access Controls

U.S. Census Bureau's information 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 U.S. Census Bureau that contains, transmits, or processes 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 U.S. Census Bureau also deploys a DLP solution as well.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

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

_X_ 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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
X	No, this system is not a system of records and a SORN is not applicable. It has been determined that Cloud Services is not a system of records. As a result, IT systems containing PII/BII that are hosted on the Cloud Services servers are governed by the SORN(s) specific to the record types stored within the IT system and must be used in accordance with the purpose(s) enumerated in the SORN.

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: Please see individual IT systems/CEN plans hosted on Cloud Services for record control schedules. RS 1 Item 23 Employee Performance File System Records; GRS 2 Item 1 Individual Employee Pay Record GRS 2 Item 8 Individual Employee Pay Record Time and Attendance Input Records GRS 3.1: General Technology Management Records GRS 3.2: Information Systems Security Records GRS 4.2: Information Access and Protection Records GRS 4.3: Input Records, Output Records, and Electronic Copies Demographic Directorate N1-29-99-5, N1-29-89-3, N1-29-87-3, N1-29-86-3, NC1-29-85-1, NC1-29-79-7 Economics Directorate N1-029-10-2, N1-029-10-3, N1-029-12-004, N1-029-10-4 Company Statistics Division N1-29-10-1 Economic Surveys Division N1-29-03-1NC1-29-80-15, NC1-29-79-4, NC1-29-78-15 NC1-29-78-8 Manufacturing and Construction Division NC1-29-81-10 Decennial Directorate Nl-29-05-01, N1-29-10-5 American Community Survey DAA-0029-2015-0001
	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.)*

	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII/BII stored/ maintained can be used to directly identify individuals
X	Quantity of PII	Provide explanation: The collection is for U.S. Census Bureau's Censuses and surveys; therefore, a severe or catastrophic number of individuals would be affected if there was loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII/BII, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the PII/BII in this IT system may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with laws. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	The PII is physically located on servers owned and managed by a third-party vendor at offsite facilities located in the United States. The third-party vendors used are Federal Risk and Authorization Management Program (FedRAMP) authorized Cloud Service Providers (CSPs).
	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 an authorized work-related 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 U.S. 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 U.S. Census Bureau limits access to sensitive information to sworn personnel (employees and contractors) who have an authorized work-related 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.