Template Version Number: 01-2021

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

Privacy Impact Assessment
for
Office of the Chief Information Officer (OCIO)
Data Ingest and Collection for the Enterprise (DICE)

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

Donna Neal Digitally signed by Donna Neal Date: 2025.01.30 16:33:02 -05'00' 2/3/25

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/OCIO Applications Development and Services Division (ADSD) Data Ingest and Collection for the Enterprise (DICE)

Unique Project Identifier: [Number]

Introduction: System Description

Provide a brief description of the information system.

The Data Ingest and Collection for the Enterprise (DICE) system is the Census Bureau's mechanism to provide a single solution for seven (7) survey data collection and data ingest activities that are common to all program areas within the Bureau. DICE replaces numerous legacy systems with new or upgraded applications that modernize and streamline how programs conduct surveys and receive external data. The goal of DICE is to produce a "system of systems" that eventually supports all Demographic and Economic surveys over the next decade, and that also provides a proven technology foundation for 2030 Census data collection.

Address the following elements:

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

DICE is a major system composed of a multiple applications.

(b) System location

DICE resides within a secured cloud environment, AWS GovCloud, which is located at 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)

DICE is housed in the FedRAMP approved AWS GovCloud. DICE interconnects with other Bureau systems in AWS GovCloud and the internal Census Bureau IT systems to leverage enterprise services (Office of the Chief Information Officer (OCIO) Data Communications, OCIO Network Services, OCIO OIS Systems) and inherits security controls provided by the Enterprise Common Control Providers (ECCP). DICE also leverages security controls available on AWS GovCloud. DICE integrates with other systems that handle tasks such as survey design, user authorization, data transmission, and operational control. These other systems include: Associate Director for Economic Programs (ADEP) Economic Applications Division Windows Applications System, ADEP Economic Census and Surveys and Special Processing, ADEP

Innovation and Technology Office (ITO), OCIO Enterprise Data Lake (EDL), OCIO ADSD Shared Services, OCIO ADSD Enterprise Applications, etc.

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

DICE is a cloud-native system used for the integrated design, delivery, and execution of surveys, censuses, and other data collection and data exchange efforts. It provides secure data collection of respondent data via the Internet for self-response, through in-person interviews, telephone interviews, and digital capture of paper survey responses. DICE simplifies the survey instrument development process by allowing reuse across the three electronic instrument collection modes: Internet, Computer Assisted Personal Interview (CAPI), and Computer Assisted Telephone Interview (CATI). DICE allows the Census Bureau to collect data more cost effectively and with a higher degree of accuracy as compared to equivalent traditional data collection methods. Standard web browser clients are used to access the DICE IT system. Members of the public accessing DICE are survey or census respondents; they authenticate to the IT system, enter response data through a series of interactive web forms, and submit survey responses.

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

Information in DICE is retrievable by a unique identifier provided to respondents.

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

Information collected from survey respondents is provided back to the survey sponsors via a secure connection. Users submit survey information via applications using secure protocols such as HTTPS.

(g) Any information sharing

Survey response data, collected by DICE, is stored in the AWS GovCloud encrypted database and deposited into secure buckets within the U.S. Census Bureau's OCIO EDL. Survey teams and other data users log in to the OCIO EDL to access their survey data, collected by DICE, for analysis and processing. Survey teams and other data users are only able to access their data via the OCIO EDL and not directly through DICE applications/databases. Each survey receives its own secure bucket within the OCIO EDL for access control purposes and survey teams/data users are only able to access their own survey data.

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

13 U.S.C. Sections 8(b), 131, 161, 141, 182, 193 and 26 U.S.C 6103(j).

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

The FIPS 199 security impact category for DICE is Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

__ This is a new information system.

____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

__X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID		i. Credit Card		m. Medical Record	
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:					

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. Sex	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
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	
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			
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	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	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email			
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.

Survey sponsors determine the appropriate method of access and/or authentication based on an analysis of sensitivity of information being collected. Some options include mailing invitations to potential survey respondents that include an access code or credential that the respondents use to login and provide the requested information, thus providing us reasonable assurance of the correct respondent. Likewise, Census has access to an extensive amount of administrative records to validate that the information being collected from respondents is accurate.

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. 0607-1024, 0607-0725
	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		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	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 (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).

DICE collects PII and BII from members of the public for several censuses and surveys conducted by the Census Bureau:

The Census Bureau is the nation's premier provider of official government statistics about the nation's people and economy. The Census Bureau's mission is established in the U.S. Constitution, and requires that it collect detailed and authoritative information about individuals, households, other residential environments (e.g., group quarters, transitory locations), and businesses. DICE is the Census Bureau's present and future mechanism for

collecting PII and BII in support of this mission. Two specific examples of data collection outcomes include:

To improve Federal services online: DICE provides a streamlined, modernized, and secure way for respondents to provide information the Census Bureau is authorized and mandated to collect. Census Bureau survey respondents can submit surveys via DICE. DICE provides a modern platform for both data collection and ingest, and will be the key entry point for all data into the Census Bureau for subsequent transfer, storage and use in the EDL. DICE refreshes legacy field and paper data collection technology with updated, flexible capabilities that reinforce the new operations and data ecosystem approach. DICE also provides functionality to interact with external data-ingest, frames and other modern data processing capabilities. DICE leverages both operations research and data science techniques to enable more efficient operations and adaptive survey design. Finally, DICE enables flexible scaling to support the diversity of the Census Bureau's data collection operations, from rapid, lightweight surveys to the decennial census, without the need for costly updates or system rebuilds. Many of the key functions provided by DICE were developed and successfully deployed in the 2020 Census, providing a strong foundation for further development and use by the entire Census Bureau.

For statistical purposes (i.e., Censuses/Surveys): DICE is intended to be the single source of data collection for the Census Bureau by FY 2033. There are over 130 surveys that will rely on the DICE applications for data collection at the end of the investment life cycle. Notable examples include:

The Economic Census is the U.S. Government's official five-year measure of American business and the economy conducted by the U.S. Census Bureau. Responding to the Census is required by law. Forms are mailed to approximately 4 million businesses, including large, medium, and small companies representing all U.S. industries. Respondents are asked to provide a range of operational and performance data for their companies.

DICE will collect data for the American Community Survey (ACS). This ongoing survey provides data annually, giving communities the current information they need to plan investments and services. Information from the survey generates data that help determine how more than $400 billion in federal and state funds are distributed each year.

DICE also collects data for the 2030 Decennial Census, including tests and the 2028 Dress Rehearsal, which involves the enumeration of over 130 million households. .

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

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution and a security operations center to monitor all Census IT system on a 24/7/365 basis.

The information in DICE is handled, retained and disposed of in accordance with appropriate federal (NARA) record schedules.

The Census Bureau conducts various surveys that study households, businesses, schools, hospitals, and more. These statistics deliver valuable information for local officials and organizations who provide resources and services to the community. If a respondent has been contacted to participate in a survey and wants to verify that it is legitimate, they can do so in numerous ways. The Census Bureau provides guidance on how to verify the legitimacy of a survey invitation at the following link: https://www.census.gov/programs-surveys/surveyhelp/verify-a-survey.html

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			
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.

(i) 6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	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: DICE is housed in the AWS GovCloud, and is provisioned and managed by the Census Bureau's Secure Cloud Team. DICE interconnects with other Bureau systems in AWS GovCloud and the internal Census Bureau IT systems to leverage enterprise services (OCIO Data Communications, OCIO Network Services, OCIO OIS Systems) and inherit security controls provided by the Enterprise Common Control Providers (ECCP). DICE also leverages security controls available on AWS GovCloud, which is FedRAMP compliant. DICE receives inbound survey sample data from other systems that handle tasks such as survey design, user authorization, data transmission, and operational control. These other systems include: ADEP Economic Applications Division Windows Applications System, Associate Director for Economic Programs (ADEP) Economic Census and Surveys and Special Processing, ADEP Innovation and Technology Office (ITO), OCIO Enterprise Data Lake, OCIO ADSD Shared Services, OCIO ADSD Enterprise Applications, etc. DICE uses a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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	X[1]	Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

[1] The survey respondent has access to their information only.

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: The privacy act statement is unique to each survey conducted by DICE. DICE also has a link at the bottom of every survey that directs the respondent to the Census Bureau Privacy Policy: https://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: In addition to the privacy act statement on each survey, DICE has a link at the bottom of every survey that directs the respondent to the Census Bureau Privacy 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.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Various surveys maintained by the DICE system are voluntary and therefore not required to provide PII/BII. A system notification message on the initial survey screen warns respondents of their consent by responding to the survey and provides the appropriate OMB information.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Some surveys and the Economic Census are mandatory as required by 13 U.S.C. Individuals are informed of this by one of the following: via Privacy Act Statements upon login, letter, interview, or during data collection.

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: Various surveys maintained by the DICE IT system are voluntary and therefore not required to provide PII/BII. A system notification message on the initial survey screen warns respondents of their consent by responding to the survey and provides the appropriate OMB information
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Some surveys and the Economic Census data maintained by the DICE system are mandatory as required by 13 U.S.C. The data are used for statistical and administrative purposes only and are exempt from consent to particular uses of PII/BII.

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: For the Economic Census and surveys maintained by the DICE system, individuals have the opportunity to provide updates to PII/BII data on the submitted survey or on the survey website.
X	No, individuals do not have an	Specify why not: For surveys that collect information for

	opportunity to review/update PII/BII pertaining to them.	statistical purposes, respondents are exempt from review/update of PII/BII unless the Census Bureau contacts them to update the information.

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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/25/2023 ☐ 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 (POAM).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)

- HSPD-12 Compliant PIV 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 that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a DLP solution as well.

DICE is housed in AWS GovCloud provisioned and managed by the Census Bureau's Secure Cloud Team. DICE interconnects with other Bureau systems in AWS GovCloud and the internal Census Bureau IT systems to leverage enterprise services (OCIO Data Communications, OCIO Network Services, OCIO OIS Systems) and inherit security controls provided by the Enterprise Common Control Providers (ECCP). DICE also leverages security controls available on AWS GovCloud, which is FedRAMP compliant.

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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies- https://www.commerce.gov/node/4937 COMMERCE/CENSUS-4, Economic Survey Collection- https://www.commerce.gov/node/4938 COMMERCE/CENSUS-5, Decennial Census Program- https://www.commerce.gov/node/4939 COMMERCE/CENSUS-7, Special Censuses of Population Conducted for State and Local Government- https://www.commerce.gov/node/4941 COMMERCE/DEPT-25, Access Control and Identity Management System- https://www.commerce.gov/node/4959
	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-0029-2015-0001 N1-029-10-2, N1-029-10-3, N1-029-12-004, N1-029-10-4 Economic Indicators Division N1-29-10-1, NC1-29-81-10 Economic Reimbursable Surveys Division N1-29-03-1, NC1-29-80-15 Demographic Surveys: N1-29-99-5, N1-29-89-3, NC1-29-85-1, N1-029-12-001 ITEMS A, B, C
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify): Secure deletion from AWS GovCloud databases.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII collected can directly identify individuals
X	Quantity of PII	Provide explanation: The collection is for Census Bureau 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, 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: PII/BII is collected by DICE for statistical purposes and to improve federal services online.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with 13 U.S.C. section 9.
X	Access to and Location of PII	Provide explanation: The PII is located on network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know including the Census Bureau regional offices and survey program offices, etc. Access is allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities. PII is also located on U.S. Census Bureau authorized vendor, such as AWS cloud 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.