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

Privacy Impact Assessment
for the
Office of the Chief Information Officer (OCIO) Enterprise Applications

Reviewed by: Donna Neal, 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: 2024.09.24 10:22:07 -04'00' 9/20/24

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 the Chief Information Officer (OCIO)
Enterprise Applications

Unique Project Identifier: 006-000401400

Introduction: System Description

Provide a brief description of the information system.

The response must be written in plain language and be as comprehensive as necessary to describe the system

The OCIO Enterprise Applications system is the functional management framework used to deliver applications to end users of the U.S. Census Bureau network. OCIO Enterprise Applications contains a variety of systems and applications that maintain or collect personally identifiable information (PII). They are:

- enterprise-level data tracking system
- general support systems for internal data management,
- transaction-based systems,
- relational database management systems; and
- web service system

Address the following elements:

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

The OCIO Enterprise Applications system is comprised of both a variety of systems and applications.

Social Media (SM) the term used for third-party websites and applications, which refers to web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on the BOC's official website.

(b) System location

OCIO Enterprise Applications reside at the following locations:

- enterprise-level data tracking system: Census Bureau Computer Center (Bowie, MD)
- general support systems for internal data management: AWS West (headquarters in Seattle, WA) and Census Bureau Computer Center (Bowie, MD)
- transaction-based system: AWS East (headquarters in Seattle, WA) and Census Bureau Computer Center (Bowie, MD)
- relational database management systems: AWS East/West (headquarters in Seattle, WA) and Census Bureau Computer Center (Bowie, MD)
- web service system: Census Bureau Computer Center (Bowie, MD)

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

OCIO Enterprise Applications systems interconnects with infrastructure services at the U.S. Census Bureau. This includes OCIO Data Communications for authentication/ telecommunication purposes, OCIO Network Services for server/storage, and OCIO Client Support Division (CSD) for laptops and workstations.

Social media, as accounted for in this Privacy Impact Assessment (PIA), are considered standalone systems which do not interconnect with any existing Bureau of Census (BOC) systems which are authorized to process PII. That said, in some cases, these tools and applications may be embedded into BOC owned and operated websites. For example, https://www.census.gov includes embedded capabilities to "Engage" the department via its primary social media outlets: Facebook, LinkedIn, X (formerly known as Twitter), and YouTube, or to share content via Facebook or X.

In addition, the OCIO Enterprise Applications systems interconnect with the following Census Bureau:

- Office of the Chief Information Officer (OCIO) Administrative Systems Vol II
- Associate Director for Demographic Programs (ADDCP) Decennial
- Office of the Chief Information Officer (OCIO) Field
- Associate Director for Demographic Programs (ADDP) Demographic Census, Surveys, and Special Processing
- Office of the Chief Information Officer (OCIO) Centurion
- Office of the Chief Information Officer (OCIO) Human Resources Applications
- Associate Director for Field Operations (ADFO) National Processing Center
- Associate Director for Research and Methodology Systems (ADRM) Cloud Research Environment
- Office of the Chief Administrative Officer (OCAO) Lenel
- Associate Director for Economic Programs (ADEP) Economic Census and Surveys and

Special Processing
- Office of the Chief Information Officer (OCIO) Commerce Business Systems
- Office of the Chief Information Officer (OCIO) Cloud Services
- Office of the Chief Information Officer Enterprise Tools and Development Services (ETDS)
- Office of the Chief Financial Officer (OCFO) Systems, Data Analysis and Business Solutions (SDB) Division Applications
- Office of the Chief Information Officer (OCIO) Office of Information Security (OIS) Systems
- Associate Director for Economic Programs (ADEP) International Trade Program Applications
- Other OCIO Enterprise Applications systems.

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

The purpose of the enterprise-level data tracking systems is to ensure data consistency, data integrity, and generate meaningful data information through data management, tracking, and reporting for Census Bureau collections. Another capability is an enterprise-wide analytics platform for surveys and censuses. This system allows statisticians within census and survey projects to perform statistical models using census and survey response data, paradata, administrative records, and many other types of data. The system will receive PII including Identifying Numbers, General Personal Data, and Work-Related Data. The PII is received from other information systems that collect, maintain and disseminate Census and Survey data.

The general support systems for OCIO Enterprise Applications provide internal data management within the Census Bureau collections. This system allows users to request access to datasets, and when approved, users are granted access to the datasets within a secure environment provisioned by the system. Census Bureau datasets are for internal use by employees and are capable of containing protected or administrative information.

The transaction-based systems within OCIO Enterprise Applications serve as the primary mechanism for operational control across surveys for data collection. The system can be considered an operational brain that determines operational workflow based on pre-existing protocols.

The relational database management systems store and retrieve data as requested by other software applications. This system provides both a testing, development, and production environment for optimum functionality.

The web service system is designed to provide a centralized and well-coordinated content

authoring and publishing system for the entire Census Bureau. This system will support the integrity of Census Bureau's branding, website look and feel as well as the business process the BOC employs to disseminate information to the general public.

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

For the enterprise-level data tracking system, authorized users can use their roles and privileges to retrieve information by personal identifiers. For the enterprise-wide analytics platform for surveys and censuses, information can be retrieved by personal identifiers, however this is not a normal function of the enterprise-wide analytics system.

For the general support systems, in regard to internal data management, information can be retrieved by personal identifiers.

For the transaction-based systems, authorized users can use their roles and privileges to retrieve information by personal identifiers.

For the relational database management system, authorized users can use their database roles and privileges to retrieve information by personal identifiers.

For the web system, when the BOC uses the Social Media/Web 2.0 (SM/WB 2.0) website or applications covered under this PIA, it does not solicit or collect PII or Business Identifiable Information (BII).

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

Information is transmitted securely via Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS).

The social media used in the form of websites, applications, and technologies may be obtained by the end user to either input general information for log in purposes or to analyze statistical data, pending the type of social media in use. Such social media involve significant participation of a non-government entity and are in a location that is not part of an official government domain.

(g) Any information sharing

The enterprise-level data tracking system does not share information. The enterprise-level analytics system is an environment for use by researchers to make decisions during the data collection phase of a survey or a Census. The system will provide the researcher with any data that they request as input and will output and send decision-based data only to other systems.

This could include things such as case level intervention codes, a stop work decision, or best time of day to contact respondents. The system does not provide a mechanism for sharing PII/BII with other systems.

The general support system shares information within the Census Bureau by querying indexed metadata and by sending email to data owners, administrators, and other application users.

The relational database management system does not share information.

The transaction-based system shares demographic survey, Decennial, and Economic Census information within the Census Bureau and with the Department of Commerce, that is used to determine new survey content, support electronic collections, for statistical purposes, and to create datasets for the Census Bureau.

The BOC does not share PII/BII that is made available through its third-party SW/W2.0 websites internally or with outside entities. Information published on third-party SM/W2.0 websites that are covered under this PIA are open for public viewing and/or commenting. Whenever someone publicly posts to BOC SM/W2.0 website, the entire contents of the posting will be publicly displayed on the BOC's SM/W2.0 website and available to all visitors of that specific website for viewing, copying, and commenting. Users are encouraged to exercise care when posting information on a public website or application.

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

5 U.S.C. 301
13 U.S.C. Chapter 9, and Sections: 6, 8(b), 9, 131, 132, 141, 161, 182, 193, 196
15 C.F.R. Part 30 and 19 C.F.R. Section 24.53
18 U.S.C. 2510-2521
26 U.S.C. 6103(j) and
Foreign Trade Statistical Regulations or its successor document, the Foreign Trade Regulations

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

The FIPS 199 security impact category for Enterprise Applications 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	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card	X	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	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	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship	X	n. Religion			

u. Other general personal data (specify): In regard to the web service system, this PII may be requested by the third-party social media application when setting up an account on its platform. BOC does not solicit any BII/PII through these applications.

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	
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	X	i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): In regard to the web services system, third-party social media application users can share/post photographs and video recordings on the applications. BOC does not solicit any of this content through these applications.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
In regard to the web service system, the BOC does not solicit, collect, maintain, or disseminate personally identifiable information from third-party social media websites or applications. However, PII or BII that is voluntarily provided by a user may be used to respond to inquiries, answer questions, or fulfill a request submitted by the user. Although the BOC does not solicit, collect, maintain, or disseminate PII/BII from visitors to these third-party social media websites or applications, it is possible for individuals to voluntarily make such information available to agencies. Typical examples of the types of PII/BII that may become available include names of individuals and businesses, images or videos, screen names, and email addresses, etc. In addition, many third-party social media websites or applications request PII/BII at the time of Registration. The process will vary across third-party social media websites or applications and often users can provide more than is required for registration. For example, users can provide such information as his or her interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contact information, and hometown. If the privacy setting on the third-party social media website or application is not restricted, such information may be made available to the BOC. Information provided to third-party social media websites or applications during registration is not collected or used by the BOC. The BOC does not ask individuals to post information on its Social Media/Website 2.0 (SM/W2.0) websites or applications.

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

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application			X		
Other (specify): In addition to information provided to the third-party social media website or application during registration, other sources of PII or BII may include screen names, information provided in comments, links, postings, and uploaded audio/video files, comments, or survey responses. Other activities conducted on the third-party social media website or application, such as "friend-ing", "following", "liking", "joining" a "group", becoming a "fan", and comparable functions, can also be a source of PII/BII in the system.					

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

The verification and validation of the accuracy of the data in the OCIO Enterprise Applications is part of the data ingest and storage process. The data used within OCIO Enterprise Applications has already been validated for accuracy before it is pulled inside the OCIO Enterprise Applications. While in use within OCIO Enterprise Applications, the data is accessible only to users that are authorized to use the data.

The initial Authorization to Operate (ATO) and the Information Systems Continuous Monitoring program provides an ongoing monitoring of data accuracy as maintained by security controls derived from NIST 800-53 Rev 5. System and Communications (SC) provides Protection of Policy and Procedures, Application Partitioning, Information in Shared Resources, Denial of Service, Information System Boundary, Transmission Confidentiality & Integrity, and Cryptographic Protection.

In addition, System and Information Integrity (SI) provides Flaw Remediation Protection, Malicious Code Protection, Inbound and Outbound Communications Traffic monitoring protection, System-Generated Alerts, etc.

In regard to the web service system, while the BOC uses social media websites and applications as platforms for communicating their message to reach as many people as possible or to target specific audiences, the BOC does not collect, maintain, or disseminate PII/BII from individuals who interact with any BOC social media website or application, nor does it solicit such information. Therefore, risks posed by data accuracy are minimal.
The BOC may use a person's screen name, email address, or other information voluntarily provided or made available by the user to respond to specific comments or questions directed to or about BOC activities, or to fulfill a request. In such situations, data is provided directly by the individual and is assumed to be accurate, timely and relevant to the specific request.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
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	X
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For research and 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).

The PII/BII maintained for administrative purposes: This IT system maintains first name, last name, address, email address, etc. to ensure that mandatory survey or statistical, information is ready for internal Census use. The information pertains and is in reference to federal employees/contractors conducting the surveys and the public.

The PII/BII maintained for statistical and research purposes: The data maintained by this IT system is collected from other IT systems that collect censuses and surveys (e.g., responses and statuses) and is used to direct data collection efforts. It is also used to inform program areas within the Census Bureau (responsible for survey and census questionnaire mail out) whom to send survey and census forms to. The IT system gathers response data from the data collection modes to send it to the survey and census processing IT systems in a standardized way. This information enables the Census Bureau to fulfill its legal obligation to provide mandated statistics. The information pertains to members of the public.

The PII/BII maintained for information sharing initiatives: This information is collected and shared within the Census Bureau and the Department of Commerce to create datasets for various types of censuses and surveys. This information enables the Census Bureau to fulfill its legal obligation to enhance its information sharing initiatives. The information pertains to members of the public.

In regard to the web service system, the BOC uses third-party social media websites and applications to collaborate and share information online by facilitating public dialogue, providing information about or from the BOC, make information and services more widely available, and to improve customer service. Our use of these third-party social media websites and applications offer important opportunities for promoting the goals of transparency, public participation, and collaboration. Through these services, people or groups can create, organize, edit, comment on, combine, and share content of mutual interest. As outlined above, the BOC does not solicit, collect, maintain, or disseminate PII/BII from visitors to these third-party social media websites or applications, although it is possible for individuals to voluntarily make such information available to agencies. Any PII or BII that is voluntarily provided by a user may be used by the Department to respond to inquiries, answer questions, or fulfill a request submitted by the user.

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. 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 information in OCIO Enterprise Applications is handled, retained, and disposed of in accordance with appropriate federal record schedules.

In regard to the web service system, there is a risk of unnecessary collection of or access to PII by BOC employees and contractors. There may be a potential for insider threat if the social media application is used in a manner that is not intended, and of any individual potentially divulging information that is sensitive. However, annual Cyber Security and Privacy Awareness Training is mandated across the bureau for annual completion. As previously stated, BOC does not collect, maintain, or disseminate PII/BII from individuals who interact with any of its SM/W2.0 websites or applications that are in a request or an inquiry to the BOC through the BOC's SM/W2.0 website, or otherwise makes such information available, the BOC may use the PII/BII provided by the user to fulfill the specific request. Although the PII/BII may be maintained by the third-party SM/W2.0 website or application, it is not maintained by the BOC. To further mitigate the risks of access to or collection of sensitive PII/BII, the BOC may, to the extent possible, and in accordance with internal policies and federal rules and regulations, choose to delete or hide comments or other user interactions when a user's sensitive information is included.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus	X		
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.[1]

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

X[2]	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[3].

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: • OCIO Administrative Systems • ADDCP Decennial • OCIO Field • ADDP Demographic Census, Surveys, and Special Processing • OCIO Centurion • OCIO Human Resources Applications • ADFO National Processing Center • ADRM Cloud Research Environment • OCAO Lenel • ADEP Economic Census and Surveys and Special Processing • OCIO Commerce Business Systems • OCIO Cloud Services • OCIO Enterprise Tools and Development Services (ETDS) • OCFO Systems, Data Analysis and Business Solutions (SDB) Division Applications • OCIO Office of Information Security (OIS) Systems • ADEP International Trade Program Applications 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

[1] The PII/BII in Web Services will not be shared.

[2] External Agencies/Entities are required to verify with the Census Bureau any re-dissemination of PII/BII to ensure consistency with the Memorandum of Understanding (MOU)/inter-agency agreement and the appropriate SORN.

[3] Web Services does not share PII/BII with external agencies.

	solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII[4].

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: Notice is provided by the individual privacy policies available on individual social media and third-party applications and capabilities used by the public to engage with BOC. As previously noted, the privacy policies of the BOC do not apply to the third-party social media websites or applications that are covered by this PIA. When visiting a BOC's third-party social media website or application.
	No, notice is not provided.	Specify why not:

[4] Web Services does not connect with or receive information from other systems.

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: For web services, PII/BII is voluntarily provided by users. BOC does not solicit, collect, or disseminate this information. This pertains to web services only.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to decline to provide PII/BII at the OCIO Enterprise Applications system level.

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: For web services, BOC may use the screen name, email address, or other information provided by application users to respond to inquiries, answer questions, or to fulfill requests submitted by the user.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to consent to particular uses of PII/BII at the OCIO Enterprise Applications system level.

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 web services, the information that is generally provided by an individual can be modified, as it is contact user log in information for setting up an account, etc.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: PII/BII is pulled from other Census Bureau Information Systems, therefore there is not an opportunity to review/update PII/BII at the OCIO Enterprise Applications 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/BII 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 18, 2023_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

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

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

For web service

- Only approved staff members from the BOC have access to manage BOC's SM/W2.0 websites and applications.
- BOC's use of third-party websites and applications have an intended purpose directly related to an agency function that supports its mission.
- Third-party website and application terms and conditions, or terms of service, which governs access to and use of such products and services are reviewed for compatibility with Federal law and regulations, or for a federal-compatible Terms of Service agreement, in accordance with Federal Acquisition Regulation Clause 48 CFR 52.212- 4(u) and OMB M-13-10, Anti-deficiency Act Implications of Certain Online Terms of Service Agreements.
  Third-party website or application privacy policies are evaluated for risks and to determine whether the website or application is appropriate for the agency's use (Initially and periodically thereafter).

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/CENSUS-2, Employee Productivity Measurement Records: https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-2 COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies: https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-3 CENSUS-4, Economic Survey Collection: https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-4 COMMERCE/CENSUS-5, Decennial Census Programs: https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-5 COMMERCE/CENSUS-7, Special Censuses of Population Conducted for State and Local Government: https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-7 COMMERCE/CENSUS-8, Statistical Administration Records Systems: https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-8 COMMERCE/CENSUS-9, Longitudinal Employer Household Dynamics System https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-9 COMMERCE/CENSUS-12, Foreign Trade Statistics: https://www.commerce.gov/opog/privacy-privacy-act/system-records-notices/system-records-notices-commerce-census-12
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1 - General Technology Management Records GRS 3.2 - Information Systems Security Records GRS 4.1 - Records Management Records GRS 4.2 - Information Access and Protection Records GRS 4.3 - Superseded by July 2017 by GRS 5.1 and GRS 5.2 (GRS 5.1 - Common Office Records & GRS 5.2 - Transitory and Intermediary Records) **Demographic Directorate** N1-29-99-5: National Prisoner Statistics Program Capital Punishment (NPS-8) Reports N1-29-89-3: Surveys Collected Under Title 15 of the U.S. Code N1-29-87-3: Survey of Fishing, Hunting and Wildlife Associated Recreation, 1980 and Later - Electronic Records (Inactive) N1-29-86-3: Current Population Survey (CPS) - Electronic Records (Inactive) NC1-29-85-1: Survey of Income and Program Participation (SIPP), 1979 and Thereafter NC1-29-79-7: Demographic Fields Area (DFA) Records Schedule **Economics Directorate** N1-029-10-2: Business Register System N1-029-10-3: Standard Economic Processing System (StEPS) N1-029-12-004: Economic Directorate Document Management System (EDMS) N1-029-10-4: Micro Analytical Database (MADb) Company Statistics Division N1-29-10-1: Survey of Business Owners & Self - Employed Persons Program Records **Economic Surveys Division** N1-29-03-1: Economic Surveys NC1-29-80-15: Surveys of Manufacturers, 1960, Sample Detail File, Backup File and Survey of Persons with College Degrees on II-A and III-A Tape (Inactive) NC1-29-79-4: Economic Census and Organization Survey Data Files , 1972 - 74 (Inactive) NC1-29-78-15: Economic Surveys Division Data Files on II-A Tape (Inactive) NC1-29-78-8: Extracts from Commodity Transportation Surveys, 1963 - 72 (Inactive) **Manufacturing and Construction Division** NC1-29-81-10: Records Schedule - Construction Statistics Division **Decennial Directorate** N1-29-05-01: Respondent Data from the 2004 Overseas Enumeration Test N1-29-10-5: 2010 Census Records Schedule **American Community Survey** DAA-0029-2015-0001: American Community Survey Records for 2007 and Thereafter
	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):			

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/BII collected can be directly used to identify individuals
X	Quantity of PII	Provide explanation: The collection is for demographic, Economic Surveys, and other surveys, and 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 act of collecting and using the PII/BII in this IT system or the PII/BII itself may result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance Title 13 collections. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: PII/BII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access is limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals. Access is only allowed by organization-owned equipment outside of the physical locations, and only with a secured connection.
	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. For the web services, there is a risk of disclosure of PII/BII by users: When interacting on a social media website (e.g. posting comments), PII/BII that users share or disclose will ordinarily become available to other users or anyone else with access to the site. Most users will likely avoid disclosing particularly sensitive or confidential PII/BII (e.g., Social Security or credit card number), which could be used by itself; or with other available information, to commit fraud or identity theft, or for other harmful or unlawful purposes. However, to help reduce those risks, the BOC will monitor postings to its authorized social media websites and applications to the extent practicable and will delete such posts of which the BOC becomes aware. Despite such efforts, the information may remain available elsewhere on the website, and others may have already viewed or copied the information. Additionally, the BOC does not request or collect any sensitive personal information, nor does it conduct any official business transactions on social media applications. Where possible, the BOC will also provide appropriate notice to users on the third-party social media website itself; warning them to avoid sharing or disclosing any sensitive PII/BII when interacting with the agency on the website. Users should also review the privacy policies of any third-party social media providers to determine if they wish to utilize that social media.

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.