Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
OCIO ADSD SharePoint

Reviewed by: Byron Crenshaw, Bureau Chief Privacy Officer

(•) Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
( ) Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

BYRON CRENSHAW Digitally signed by BYRON CRENSHAW
Date: 2022.03.10 16:25:29 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/OCIO ADSD SharePoint

Unique Project Identifier: [Number]

Introduction: System Description

Provide a brief description of the information system.

Microsoft SharePoint Online and SharePoint 2016, which makes up Office of Chief Information Officer (OCIO) Application Development and Services Division (ADSD) SharePoint, are a collection of Web-based tools and technologies that help users store, share, and manage digital information within an organization. The SharePoint platform allows developers to create sites for various purposes such as document management, workflow automation, web portals, intranets, as well as others. SharePoint consists of hundreds of site collections throughout the U.S. Census Bureau.

SharePoint (internal) may be used to collect or store personally identifiable information (PII)/business identifiable information (BII) information for administrative purposes for account management for employees and contractors. To do so, SharePoint collects information on employees and contractors for account purposes. SharePoint (external) may be used to collect or store PII/BII information from members of the public for sharing initiatives to encourage collaboration between other federal agencies, universities, research agencies, etc. and the Census Bureau.

Address the following elements:

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

SharePoint is a major application that consists of two environments, an on-premise environment known as SharePoint 2016 and a cloud environment known as SharePoint Online.

(b) System location

The on-premise environment, SharePoint 2016, resides at the Bowie Computing Center in Bowie, Maryland. The cloud environment, SharePoint Online, resides in Microsoft O365 Government Community Cloud (GCC) located in Redmond, Washington.

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

SharePoint interconnects with infrastructure services at the U.S. Census Bureau. This includes Data Communications system for authentication/telecommunication purposes, Network Services system for server/storage/authentication, and Client Services system for laptops and workstations.

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

Microsoft SharePoint Online and SharePoint 2016 are a collection of Web-based tools and technologies that help users store, share, and manage digital information within an organization. The SharePoint platform allows developers to create sites for various purposes such as document management, workflow automation, web portals, intranets, as well as others. SharePoint consists of hundreds of site collections throughout the U.S. Census Bureau. Each site collection has a site collection administrator and/or site owner. The information on each site is managed by site collection administrators/site owners and are governed by a governance policy.

SharePoint solutions for internal users will utilize Network Services' Windows Active Directory for identification and authentication of users.

SharePoint solutions for external users will utilize the OCIO Data Communications Census Public Access Security System (C-PASS). C-PASS collects and requests account information, as well as user passwords. C-PASS focusses on meeting requirements to allow external users to securely authenticate and consume Census controlled data and services. The system provides supporting services required to allow controlled access to Census data, which is only available to approved individuals.

SharePoint hosts the Commerce Accommodation Tracking System (CATS). The purpose of the CATS is to record, track, and manage reasonable accommodation requests submitted by Department of Commerce (DOC) employees. The CATS collects personally identifiable information (PII) including names, telephone number, and email address in order to track and process reasonable accommodation requests for contractors and employees with temporary or permanent disabilities. Although the tracking system does not request specific medical information, individuals may voluntarily enter specific medical information about themselves regarding their medical disabilities. The information entered is used solely by appropriate DOC employees who have a business need to know in the performance of official duties to satisfy reasonable accommodation requests.

In addition, SharePoint will host an electronic signature application. The employees will use their personal identity verification (PIV) cards to sign electronic documents. The application prompts employees to enter their personal identification number (PIN), and it will use the public

certificate stored in their PIV cards to sign the electronic documents. This privacy impact assessment reflects all PII that is requested by the Census Bureau that will be use, dissemination, or storage within this IT system.

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

Authorized and authenticated Census employees can retrieve information by identifiers such as name and email address.

(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).

(g) Any information sharing

Internal SharePoint: The SharePoint team and system administrators do not share information with other IT systems. However, there is information sharing internal to SharePoint, as it was created for collaboration purposes. Census employees, outside of the system administrators and SharePoint program area, are able to share information with one another for collaboration purposes.

Information within the CATS is shared with appropriate DOC employees who have a business need to know in order to process reasonable accommodation requests.

External SharePoint Sites: Information is also shared with approved, external, individuals that need access to Census data via an extranet SharePoint site. This may include other DOC bureaus and operating units, universities, etc. The access to the external SharePoint site is controlled and the user must be approved before accessing the information.

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

5 U.S.C. 301, 5 U.S.C. 29 U.S.C. 791, 41 U.S.C. 433(d), 44 U.S.C. 3101

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

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		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	X[1]
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Marital Status	

[1] Although the tracking system does not request specific medical information, individuals may voluntarily enter specific medical information about themselves regarding their medical disabilities. The information entered is used solely by appropriate Department of Commerce employees who have a business need to know in the performance of official duties to satisfy reasonable accommodation requests.

f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

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

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

SharePoint consists of hundreds of site collections throughout the U.S. Census Bureau. Each site collection has a site collection administrator/site owner. The accuracy of the information on each site is managed by site collection administrators and subsite owners and governed by by a governance policy. The subsite owner is the registered owner of a site within a site collection and has the full control permission level on the site they own. A subsite owner does not have access to content in any site in the site collection, other than the site they own, unless they are given explicit permissions to the other site.

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		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

SharePoint (internal) may be used to collect or store PII/BII information for administrative purposes:
SharePoint provides account management for employees and contractors. SharePoint collects information on employees and contractors for account purposes. The PII collected is shared only with U.S. Census Bureau employees who have a business need to know.

SharePoint (external) may be used to collect or store PII/BII information from members of the public for sharing initiatives:
The external SharePoint platform is used to encourage collaboration between other federal agencies, universities, research agencies, etc. and the Census Bureau. Individuals from federal agencies, research agencies, and universities that will be using the external SharePoint sites will go through an approval process before they can be granted access to a specific portion of the extranet SharePoint site. They are authorized using C-PASS and will login via a username and password. The PII collected for this purpose includes name, phone number,

and email address from individuals that need access to the external SharePoint sites. The PII collected is shared only with DOC employees who have a business need to know.

Information within the CATS is shared only with appropriate DOC employees who have a business need to know.

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

No Title data may be stored in any SharePoint site collection, subsite, or any Power Platform applications without the explicit authorization of the Governance Council. No Title data may be stored in any SharePoint Online (Cloud) site collection or subsite. Any PII, or in the case of Title data authorization by the Council is granted, Title 26, 13, or 5 data stored in a Census Bureau SharePoint site must comply with Census Bureau policy on PII and Title data. The site collection owner will keep a list of all
sites under their jurisdiction containing PII or Title data, and will certify to the Council on an annual basis, the sites' compliance with the policy. Additionally, a site collection administrator will be responsible for performing random checks for PII and Title Data on sites under their jurisdiction in the SharePoint Online environment. The Council will periodically review individual sites to monitor for compliance with this policy.

The subsite owner, in conjunction with the site collection administrator and the site owner is responsible for compliance with governance policy for their site within a site collection. Enterprise wide SharePoint training provides to all site collection administrators to make sure that they familiar with the SharePoint processes and compliance with the governance policy. In addition, the subsite owner, in conjunction with the site collection administrator, is also the designated audit log reviewer for the site and must review site audit logs on at least a monthly basis for indications of inappropriate or unusual activity. Any indications of such behavior must be reported to the site collection administrator and the Enterprise Content Management Branch Security Officer for further review and action.

The information in SharePoint is handled, retained and disposed of in accordance with appropriate federal 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	X		
Federal agencies			
State, local, tribal gov't agencies			
Public	X[2]		
Private sector	X[2]		
Foreign governments			
Foreign entities			

[2] The external SharePoint platform is used to encourage collaboration between other federal agencies, universities, research agencies, etc. and the Census Bureau. Individuals from federal agencies, research agencies, and universities that will be using the external SharePoint sites will go through an approval process before they can be granted access to a specific portion of the extranet SharePoint site. They are authorized using Data Communications' C-PASS and will login via a username and password.

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. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: SharePoint interconnects with infrastructure services at the U.S. Census Bureau. This includes Data Communications system for authentication/telecommunication purposes, Network Services system for server/storage/authentication, and Client Services system for laptops and workstations. SharePoint 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 in transit and at rest, and various physical controls at Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise 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[3]	Government Employees	X
Contractors	X		
Other (specify):			

[3] The external SharePoint platform is used to encourage collaboration between other federal agencies, universities, research agencies, etc. and the Census Bureau. Individuals from federal agencies, research agencies, and universities that will be using the external SharePoint sites will go through an approval process before they can be granted access to a specific portion of the extranet SharePoint site. They are authorized using Data Communications system CPASS and will login via a username and password.

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.html	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Employees on the internal SharePoint sites may wish to upload a photograph to their user profile. Photographs are not required, this is optional, and they may wish to decline upload.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: SharePoint is not used for data collection, it is a repository of data. SharePoint pulls user profile information from Network Services system Lightweight Directory Access Protocol (LDAP) therefore users do not have an opportunity to decline to provide PII/BII at the SharePoint level. For external users, there is not an ability to decline to provide PII at the SharePoint level. Account information is provided at the Data Communications system level via C-PASS.

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: Employees on the internal SharePoint sites may wish to upload a photograph to their user profile. Photographs are not required, this is optional. Therefore, users imply consent when uploading their photo, however they may wish to decline upload altogether.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: SharePoint is not used for data collection, it is a repository of data. SharePoint pulls user profile information from Network Services system LDAP therefore users do not have an opportunity to consent to uses at the SharePoint level. For external users, there is not an ability to consent to uses of PII at the SharePoint level. Account information is provided at the Data Communications system level via C-PASS.

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: Photographs can be reviewed/updated by the employees. Photographs are not required, this is optional.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: SharePoint is not used for data collection, it is a repository of data. SharePoint pulls user profile information from Network Services system LDAP therefore users do not have an opportunity to consent to uses at the SharePoint level. For external users, there is not an ability to consent to uses of PII at the SharePoint level. Account information is provided at the Data Communications system level via C-PASS.

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:
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 22, 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.
	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).*

The SharePoint system uses Account Management security controls to allow the proper access to users and system administrators. The system uses auditing controls to provide accountability of who, what, when, where, how, a service or a person is accessing the system. The system also uses change management for updates, and upgrades to the system. Lastly, the system uses encryption to make sure the data is secure inflight and at rest. 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 I Prevention Systems (IDS I JPS)
- 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 B11/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. Census 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)?

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

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies: https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html COMMERCE/DEPT-25, Access Control and Identity Management System: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html OPM/GOVT-7, Applicant Race, National Origin, and Disability Stats Records: https://www.osec.doc.gov/opog/PrivacyAct/sorns/GOV-Wide/OPM-GOVT-7-opm-sorn-govt-7-applicant-race-sex-national-origin-and-disability-status-records.pdf
	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 2.3, 3.1, 3.2, 5.1 and 5.2
	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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

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

X	Identifiability	Provide explanation: PII/BII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
X	Quantity of PII	Provide explanation: SharePoint is utilized to collect Census Bureau Census and survey information, therefore, a serious or substantial number of individuals would be affected if there was a loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII/BII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
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 serious harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII/BII collected is required to be protected in accordance with: 13 U.S.C 9
X	Access to and Location of PII	Provide explanation: The PII is located on computers (including laptops) and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know 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 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.