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

Privacy Threshold Analysis
for
OCIO ADSD SharePoint

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau OCIO ADSD SharePoint

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*
The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 purpose that the system is designed to serve

The purpose of SharePoint is for administrative matters and to promote information sharing activities.

e) The way the system operates to achieve the purpose

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

SharePoint (internal) may be used to collect or store PII/business identifiable information (BII) information for administrative purposes: SharePoint provides account management for employees and contractors. 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: 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.

The CATS collects 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

g) Identify individuals who have access to information on the system

Census Bureau employees and contractors have access to the internal SharePoint solution. 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.

h) 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.

i) How information is transmitted to and from the system

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

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

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. *Continue to answer questions and complete certification.*

__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. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

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

__X__ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Other Federal Government personnel
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

__X__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

___x__ The criteria implied by one or more of the questions above **apply** to the SharePoint and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the SharePoint and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer Name: James Keith Office: Office of Information Security Phone: 202-603-4576 Email: james.j.keith@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: JAMES KEITH Digitally signed by JAMES KEITH Date: 2023.02.13 14:15:54 -05'00' Date signed:	**Chief Information Security Officer** Name: Beau Houser Office: Office of Information Security Phone: 301-763-1235 Email: beau.houser@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2023.02.28 10:53:18 -05'00' Date signed:
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: Byron.crenshaw@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.03.06 16:51:30 -05'00' Date signed:	**Authorizing Official** Name: Luis J. Cano Office: Office of the Chief Information Officer Phone: (301) 763-3968 Email: luis.j.cano@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2023.02.28 16:02:52 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: Byron.crenshaw@census.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.03.06 16:54:23 -05'00' Date signed:	