

U.S. Department of Commerce

U.S. Census Bureau



Privacy Threshold Analysis for the CEN 26 SharePoint

U.S. Department of Commerce Privacy Threshold Analysis

Census Bureau/CEN26 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 from 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 and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

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).

a) *Whether it is a general support system, major application, or other type of system*
Microsoft SharePoint is a collection of Web-based tools and technologies that help users store, share, and manage digital information within an organization.

b) *System location*
Bowie and Greenbelt, Maryland

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
SharePoint solutions for external users will utilize the 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 solutions for internal users will utilize Windows Active Directory for identification and authentication of users.

d) *The purpose that the system is designed to serve*
SharePoint is intended for all Census hosted SharePoint solutions, for internal (Census Bureau Only) and external (Non-Census Bureau) customers.

The SharePoint platform allows developers to create websites for various purposes such as document management, workflow automation, web portals, intranets, as well as others.

CEN26 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 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 Department of Commerce employees who have a business need to know in the performance of official duties to satisfy reasonable accommodation requests.

e) The way the system operates to achieve the purpose

Internal (Census Bureau Only) and External (Non-Census Bureau SharePoint solution platforms will be similar, but differ in the way that they identify and authenticate users. SharePoint solutions for external users will utilize the Census Public Access Security System (C-PASS) to request accounts and manage accounts, as well as their passwords. The C-PASS system is an accredited system within the CEN01 C&A Package. Internal SharePoint solutions will utilize Windows Active Directory for identification and authentication of users.

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

Some examples of survey and census information maintained by this system are personal names, personal addresses, personal contact information (telephone numbers, email address), business information, occupation, medical information, tax information, etc. The systems reside in Census Bureau's Bowie Computing center. The components that collect PII/BII do not reside in the cloud.

In addition, CEN26 will host an electronic signature application. The employees will use their PIV cards to sign electronic documents. The application prompts employees to enter their PIN, and it will use the public certificate stored in their PIV cards to sign the electronic documents.

g) Identify individuals who have access to information on the system
Census Federal, Contractual Workers, and OGC workers

h) How information in the system is retrieved by the user
Secured Laptops, PC's, or Servers

- i) How information is transmitted to and from the system*
-Intrusion Detection | Prevention Systems (IDS | IPS)
-Firewalls
-Mandatory use of HTTP(S) for Census Public facing websites

- Intranet Sites
- Use of trusted internet connection (TIC)

Questionnaire:

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

_____ 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 (version 01-2015 or later). *Skip questions and complete certification.*

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. *Please describe the activities which may raise privacy concerns.*

___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 about: *(Check all that apply.)*

- ___ Companies
- ___ Other business entities

___x ___ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

___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
- ___ 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 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.

4c. 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.

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, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

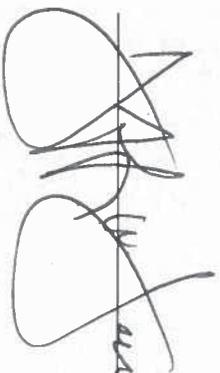
 X I certify the criteria implied by one or more of the questions above **apply** to CEN26 Sharepoint and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): David Peters

Signature of or SO:  Date: 5/14/19

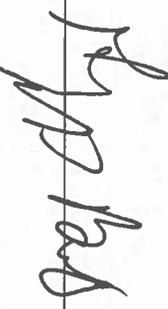
Name of Chief Information Security Officer, Acting: Jeffery W. Jackson

Signature of CISO:  Date: 7/1/2019

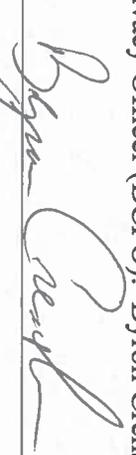
Name of Technical Authorizing Official (AO): Kevin B. Smith

Signature of AO:  Date: 6-26-19

Name of Business Authorizing Official (AO): Greg D. Bailey

Signature of AO:  Date: 7/1/20

Name of Bureau Privacy Officer (BCPO): Byron Crenshaw

Signature of BPO:  Date: 7/14/19