

U.S. Department of Commerce

U.S. Census Bureau



Privacy Threshold Analysis
for the
CEN33 DataWeb

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/CEN33 DataWeb

Unique Project Identifier: N/A

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.*

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

TheDataWeb is a distributed data dissemination system that provides easy access to data from disparate sources.

b) System location

TheDataWeb systems are located at the Bowie Computer Center. The center is a single-story structure located at the University of Maryland Science and Technology Center in Bowie, MD.

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

TheDataWeb is a standalone system.

d) The purpose that the system is designed to serve

TheDataWeb brings together demographic, economic, environmental, health and other datasets in an environment of data intelligence and analysis, empowering effective decision-making through DataFerrett and the Census Data Application Programming Interface (API), both of which are public facing.

e) The way the system operates to achieve the purpose

TheDataWeb system is a Web Application. A typical transaction is a user request made through DataFerret for a specific instance(s) of a specific dataset(s) that will be used for comparative analysis, data visualization and/or graphic representation.

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

The public data in TheDataWeb includes general personal data (GDP) such as gender, age, race, etc., as noted under "General Personal Data for Public Dissemination." This GDP includes aggregated data and microdata that have been processed through disclosure avoidance procedures; individual personal data cannot be discerned from this data. This characteristic of GDP stored within TheDataWeb for the purpose of public dissemination ensures that PII/BII will not be accessed via TheDataWeb.

The data available through TheDataWeb is public data that does not contain any Title 5, Title 13, Title 15, or Title 26 data. There is no PII or BII disseminated through TheDataWeb. The only information that is shared is that received by TheDataWeb from data owners who have validated that titled data has been excluded prior to any transfer to TheDataWeb. The data validation performed by data owners confirms that the release of public data complies with all disclosure avoidance rules.

TheDataWeb collects internal microdata (as noted under "General Personal Data for Internal Systems Use Only") related to the Census Open Data API key registration. This microdata, which may include email addresses, employer/organization information, IP address, data/time of access, and number/type of queries run, is stored for internal system use only and is accessible only by US Census Bureau personnel specifically authorized by CEN33. Internal microdata is never released to the public or shared with other government agencies or organizations.

TheDataWeb also maintains internal microdata (as noted under "General Personal Data Maintained for Access by Authorized Internal Analysts Only") that include data that has not been processed through disclosure avoidance procedures, unedited data, and processing variables. This information is only available to internal Census Bureau analysts that have authorized access by TheDataWeb and the data owner(s). Internal microdata is never released to the public or shared with other government agencies, organizations, or Census personnel that have not been authorized access.

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

The public data in TheDataWeb can be accessed by the public through its web interface.

Authorized US Census Bureau employees and contractors can access the internal microdata in TheDataWeb. This information is only available to internal Census Bureau analysts that have authorized access by TheDataWeb and the data owner(s). Internal microdata is never released to the public or shared with other government agencies, organizations, or Census personnel that have not been authorized access.

h) How information in the system is retrieved by the user

User requests are made after successfully logging into DataFerrett by using an email address as a user id. Such emails are never associated with specific individuals or PII/BII and are stored within TheDataWeb for use in delivering system announcements and/or updates only.

i) How information is transmitted to and from the system

TheDataWeb is a web application. Access to TheDataWeb application data is enabled through its web sites and APIs. Data for TheDataWeb is provided internally to the system, from internal Census program sources.

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. Sec: 44. U.S.C. § 3502(8).

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 (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 (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.*

_____ 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

_____ 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...”

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

____ DOC employees

____ 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?

____ 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

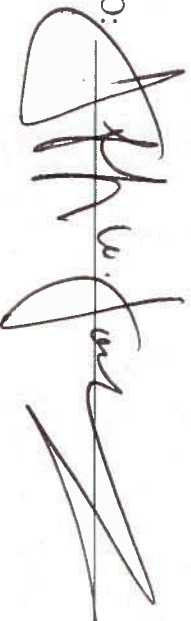
X I certify the criteria implied by one or more of the questions above **apply** to the CEN33 DataWeb and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the CEN33 DataWeb and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Robert Sienkiewicz

Signature of SO:  Date: 4/24/19

Name of Chief Information Security Officer (CISO): Jeffery W. Jackson

Signature of CISO:  Date: 6/12/19

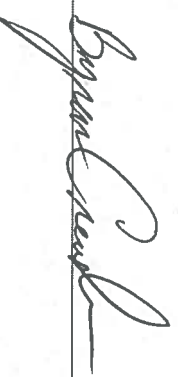
Name of Authorizing Official (AO): John L. Eltinge

Signature of AO:  Date: 7/14/2019

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO:  Date: 6/24/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO:  Date: 7/30/19