

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



Privacy Threshold Analysis
for
CEN15 Centurion

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/CEN15 Centurion

Unique Project Identifier: 006-000401700

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:

The CEN15 IT system includes Centurion. This is a web-based application used for the design, delivery, and execution of surveys, censuses, and other data collection and data exchange efforts over the Internet. Centurion allows the Census Bureau to collect data more cost effectively and with a higher degree of accuracy as compared to equivalent traditional data collection methods.

- Information collected via the Centurion IT system includes data covered by Title 13 and Title 26 collection authorities for demographic and economic surveys. Standard web browser clients are used to access the Centurion IT system. Members of the public accessing Centurion are survey or census respondents. Information collected via Centurion includes, but is not limited to, names, telephone numbers, email addresses, etc.

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*

Major application/web application

b) *System location*

Bowie Computer Center (BCC)

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

Centurion interconnects with two systems currently to provide data collected back to survey sponsors:

- Bureau of Industry and Security (BIS) BECCI-2 – BECCI-2 provides the data exchange support that BIS uses to communicate with other federal agencies.
- Application Development and Services Division (ADSD) Field Systems Development Master Control System (MCS) - MCS is the central entry and exit point for the ADSD field data collection system for Current Demographic and Economic Survey operations. MCS securely transfers these data collection files to Census staff across the enterprise.

d) The purpose that the system is designed to serve

Survey respondents access the Centurion web application on the internet using a secure web browser.

e) The way the system operates to achieve the purpose

They authenticate to the IT system, enter response data through a series of interactive web forms, and submit survey responses.

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

PII, BII, Title 13, Title 26

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

Information on the system is only limited to a handful of Centurion administrative users.

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

The Centurion application allow survey sponsors, both internally (program area sponsors) and externally (sponsors of reimbursable surveys), access to their specific data. In other words, the data is shared by allowing Census Bureau personnel and data sponsors access to the data. Census Bureau personnel may have to process some data for external survey sponsors. The Centurion system automatically generates output files for each survey in one of many supported output formats. Output files are generated on a predetermined schedule and either delivered to the Bureau's MCS system where internal Bureau survey areas can then pick up their files or are delivered directly to where internal Bureau survey areas servers using the secure protocol.

i) How information is transmitted to and from the system

Information collected from survey respondents is provided back to the survey sponsors through Secure File Transfer (SFTP).

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.*

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 PTA 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 CEN15 Centurion System 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 CEN15 Centurion and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): David Peters Glenn Fanes Acting for Dave Peters

Signature of SO: [Signature] Date: 4/25/19

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

Signature of CISO: [Signature] Date: 25 Apr 2019

Name of Authorizing Official (AO): Kevin Smith

Signature of AO: [Signature] Date: 6/10/19

Name of Authorizing Official (AO): Greg Bailey [Signature]

Signature of AO: [Signature] Date: 6/11/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw Byron Crenshaw

Signature of BPO: [Signature] Date: 6/26/19