Version Number: 01-2017

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

Privacy Threshold Analysis
for the
CEN31 Administrative Systems Vol. II

U.S. Department of Commerce Privacy Threshold Analysis

U.S Census Bureau/ CEN31 Administrative Systems Vol. II

Unique Project Identifier: 006-000403600

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:

1. *Whether it is a general support system, major application, or other type of system*
   Major applications

2. *System location*
   CEN31 components are located at the Bowie Computing Center

3. *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
   CEN 31 applications interconnect with CBS.

4. *The purpose that the system is designed to serve*
   Various services for Census employees: forms processing, mail services, commuting services, conference room reservations, library card catalog, and event management.

5. *The way the system operates to achieve the purpose*
   Access is available to all census employees using the web interfaces.

6. *A general description of the type of information collected, maintained, use, or disseminated by the system*
   - CENdocS (Census Document System) is the web-based system for requesting Forms design services from Forms and Mail Management Branch, Publications and graphics services from Publications Services Branch, and Printing services through commercial vendors). It is integrated with the CBS system.
   - ACSD Service Center which includes Records Management.
   - Conference Reservation System which allows employees to reserve rooms.
   - Share-a-Ride which is a database/LDAP Web application used by Census employees to gather information to form car-pools and van-pools.
   - Library Management System includes the online library system and card catalogue. The library staff is the primary user of the Library Management

System for checking in and checking out books. It is also a repository of online books in PDF format.

- Environment Monitoring System is a software/hardware solution to monitor the temperature/ humidity in the HQ Data Centers.
- Census Mail Metering System is a collection of mail metering stations located at Census headquarters and the 6 regional offices that are used to place postage on outgoing USPS and FedEx mail pieces or parcels. The transactions are recorded and later imported into the CBS Postal System.
- Event Management System (EMS) professional application is used to manage reservations for the first floor conference rooms, training rooms, and the auditorium.

7. *Identify individuals who have access to information on the system*
   All Census employees

8. *How information in the system is retrieved by the user*
   HTTPS

9. *How information is transmitted to and from the system*
   HTTPS

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.*

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.

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, 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 CEN31 Administrative Systems Vol. II 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 SO: _____ Date: 5/29/18

Name of Chief Information Security Officer (CISO): Timothy Ruland

Signature of CISO: _____ Date: 6/6/18

Name of Authorizing Official (AO): Kevin Smith

Signature of AO: _____ Date: 6/13/18

Name of Authorizing Official (AO): David Ziaya

Signature of AO: David R Ziaya Date: 6/15/18

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BCPO: _____ Date: 6/26/18