Version Number: 01-2015

U.S. Department of Commerce
Bureau of the Census

Privacy Threshold Analysis
for
CEN16 Network Services

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/ CEN16 Network Services

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 and its purpose 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).

The CEN16 Network Services General Support System (GSS) consists of servers that are primarily managed by the Computer Services Division (CSvD) to support the Census Bureau's mission to collect United States (U.S.) statistical data. CSvD's mission is to provide the Census Bureau and other customers with a world-class computer center using "best practices" and state-of-the-art technology to monitor systems, communications, and applications. In addition, CSvD ensures the delivery of expert systems administration services and the functionality of a stable, fault tolerant, and secure computing facility. The CEN16 servers are located at the U.S. Census Bureau's Bowie Computer Center (BCC), Headquarters, and the Regional Offices. The Bowie Computer Center located in Bowie, Maryland provides the Bureau with a reliable, state-of-the-art processing facility. The mission of the Bureau's BCC requires that critical processing operations are available on a 24-hour, 7-days-a-week basis.

The CEN16 Network Services General Support System stores and maintains PII/BII for all of the CEN PLANS located in the Census Bureau. Access to this data is only accessible by CEN16 on the administrative level. CEN16 does not perform the dissemination. The systems hosted on CEN16 servers perform the dissemination.

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):					

____x☐ This is an existing information system in which changes do not create new privacy risks. *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.

__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.)."

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

___x_☐ Companies

__x__☐ 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..."

___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__☐ 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.

Version Number: 01-2015

CERTIFICATION

__x__☐ I certify the criteria implied by one or more of the questions above **apply** to CEN16 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): _____

Signature of SO: KENNETH BOYD Digitally signed by KENNETH BOYD Date: 2019.06.04 12:00:03 -04'00' Date: _____

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

Signature of CISO: _____ Date: 7/5/2019

Name of Business Authorizing Official (AO): _____

Signature of AO: _____ Date: 7/9/19

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO: _____ Date: 7/9/19

Name of Bureau Chief Privacy Officer (BCPO): Byron Crenshaw

Signature of BCPO: _____ Date: 7/9/19