

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



**Privacy Threshold Analysis**  
**for the**  
**CEN 16 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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

CEN16 Network Services consists of servers that are primarily managed by the Computer Services Division (CSvD). A server is a computer or operating system that provides resources, data, services, or programs to other computers, known as clients, over a network.

CEN16 supports 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.

CEN16 Network Services hosts Census Bureau IT systems that may use, store, and maintain PII/BII received from the public through surveys, censuses, or from other IT systems that use, store and maintain other PII including personnel data, etc. Access to this data is only accessible by CEN16 server administrators. CEN16 does not perform dissemination of information; the IT systems hosted on CEN16 servers perform information dissemination.

*(a) Whether it is a general support system, major application, or other type of system*  
General Support System

*(b) System location*

The CEN16 servers are located at the U.S. Census Bureau's Bowie Computer Center (BCC), Headquarters, and the Regional Offices.

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

CEN16 connects with and hosts all Census Bureau IT systems that store and maintain information. Authentication information is received from CEN01 Data Communications.

*(d) The purpose that the system is designed to serve*

CEN16 is designed to serve two purposes:

- For Administrative Matters; Authentication information is received from CEN01 for Census Bureau employees and contractors for authentication purposes. This is used to provide access to the servers.
- Other; PII/BII received from other IT systems covered by other CEN plans is maintained on CEN16 server infrastructure for Storage Area Network (SAN) storage; data is not disseminated. This data refers to all PII/BII maintained by other Census Bureau information systems – including data received from the public through surveys, federal employees, contractors, foreign nationals, and visitors.

*(e) The way the system operates to achieve the purpose*

CEN16 Network Services consists of servers that are primarily managed by the Computer Services Division (CSvD). The servers operate by hosting IT systems covered by other CEN plans. The PII/BII is maintained on CEN16 server infrastructure for Storage Area Network (SAN) storage; data is not disseminated.

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

CEN16 Network Services hosts Census Bureau IT systems that may use, store, and maintain PII/BII received from the public through surveys, censuses, or from other IT systems that use, store and maintain other PII including personnel data, etc.

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

U.S. Census Bureau employees and contractors have access to CEN16.

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

Information is not retrieved at the server level by personal identifier, but may be retrieved by the hosted IT systems. Therefore, CEN16 is not a Privacy Act system of records.

The information retrieved from IT systems containing PII/BII that are hosted on the CEN16 servers are governed by the system of record notice(s) (SORN(s)) specific to the record types stored within the IT system and must be used in accordance with the purpose(s) identified in the SORN.

*(i) How information is transmitted to and from the system*

No PII/BII is transmitted by the CEN16 servers or operating system; only the IT systems hosted on the servers transmit information.

**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.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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).  
*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 01-2017 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. *(Check all that apply.)*

<b>Activities</b>			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

  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.

☐ No, this IT system does not collect any BII.

## 4. Personally Identifiable Information (PII)

## 4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

☒ DOC employees

☐ National Institute of Standards and Technology Associates

☒ Contractors working on behalf of DOC

☒ Other Federal Government personnel

☒ 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 Social Security numbers (SSNs), including truncated form?

☒ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

SSN could reside within IT systems, residing on CEN16 server infrastructure. Other PIAs for IT systems hosted on CEN16 servers will contain SSN justifications, as applicable.

Provide the legal authority which permits the collection of SSNs, including truncated form. As a result, IT systems containing PII/BII that are hosted on the CEN16 servers are governed by the SORN(s) specific to the record types stored within the IT system and must be used in accordance with the purpose(s) enumerated in the SORN. The legal authorities for each IT system, containing PII/BII hosted on the CEN16 servers, can be located in its respective SORN.

☐ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d 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 CEN16 Network Services 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): Kenneth R. Boyd

Signature of SO: **KENNETH BOYD**  Digitally signed by KENNETH BOYD  
Date: 2020.08.24 17:22:54 -04'00' Date: \_\_\_\_\_

Name of Chief Information Security Officer (CISO): Beau Houser

Signature of CISO: **BEAU HOUSER**  Digitally signed by BEAU HOUSER  
Date: 2020.09.15 09:56:01 -04'00' Date: \_\_\_\_\_


Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: **BYRON CRENSHAW**  Digitally signed by BYRON CRENSHAW  
Date: 2020.09.22 12:28:18 -04'00' Date: \_\_\_\_\_


Name of Technical Authorizing Official (TAO): Kevin Smith

Signature of TAO: **KEVIN SMITH**  Digitally signed by KEVIN SMITH  
Date: 2020.09.17 12:05:20 -04'00' Date: \_\_\_\_\_

Name of Business Authorizing Official (BAO): Gregg D. Bailey

Signature of BAO: **GREGG BAILEY**  Digitally signed by GREGG BAILEY  
Date: 2020.09.21 12:01:44 -04'00' Date: \_\_\_\_\_

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: **BYRON CRENSHAW**  Digitally signed by BYRON CRENSHAW  
Date: 2020.09.22 12:41:17 -04'00' Date: \_\_\_\_\_