

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



**Privacy Threshold Analysis**  
**for the**  
**CEN 18 Enterprise Applications**

## U.S. Department of Commerce Privacy Threshold Analysis

### U.S. Census Bureau

**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 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).

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

The CEN18 Enterprise Applications system is the functional management framework used to deliver applications to end users of the U.S. Census Bureau network.

*b) System location*

Bowie and Greenbelt, Maryland

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

The IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII: CEN01, CEN03, CEN04, CEN05, CEN07, CEN08, CEN10, CEN11, CEN13, CEN16, CEN17, CEN24, CEN26, and CEN33

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

Deliver applications and information to end users of the U.S. Census Bureau network and customers outside the network.

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

CEN 18 Enterprise Applications provide a definitive source for application support by supporting existing technologies and methodologies and investigate and promote the use of the new technologies. CEN 18 Enterprise Applications are a principal provider for computer related education and information.

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

Some examples of survey and census information maintained by this system are personal names, personal addresses, personal contact information (telephone numbers, email address), business information, occupation, medical information, tax information, etc. The systems reside in Census Bureau's Bowie Computing center. The components that collect PII/BII do not reside in the cloud.

The CEN18 Enterprise Applications system includes several applications that maintain or collect personally identifiable information (PII). These applications are:

- an enterprise-level data tracking system;
- a general support system for internal data management,
- a transaction-based system
- a relational database management system, and
- a concurrent analysis and estimation system (CAES)

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

Census Federal and Contractual Workers

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

Secured Laptops, PC's, or Servers

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

-Intrusion Detection | Prevention Systems (IDS | IPS)

-Firewalls

-Mandatory use of HTTP(S) for Census Public facing websites

-Intranet Sites

-Use of trusted internet connection (TIC)

**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.*
- 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

\_\_\_\_\_ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] 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 Information System Security Officer (ISSO) or System Owner (SO):

\_\_\_\_\_ James Keith \_\_\_\_\_

Signature of ISSO or SO: \_\_\_\_\_  \_\_\_\_\_ Date: 3/26/18

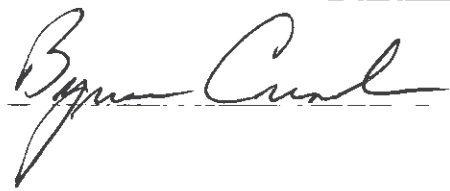
Name of Information Technology Security Officer (ITSO): Timothy P Rolano

Signature of ITSO: \_\_\_\_\_  \_\_\_\_\_ Date: 4/3/18

Name of Authorizing Official (AO): Kevin Smith

Signature of AO: \_\_\_\_\_  \_\_\_\_\_ Date: 4/3/18

Name of Bureau Chief Privacy Officer (BCPO): \_\_\_\_\_

Signature of BCPO: \_\_\_\_\_  \_\_\_\_\_ Date: 4/17/18