

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



**Privacy Threshold Analysis  
for the  
CEN35 EAD Windows Applications System**

**U.S. Department of Commerce Privacy Threshold Analysis**  
**U.S. Census Bureau/CEN35 EAD Windows Applications System**

**Unique Project Identifier: 006-00040070**

**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*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

**Description of CEN35 EAD Windows Applications System:**

- a. CEN35 EAD Windows Applications System is a general support system.
- b. CEN35 EAD Windows Applications System servers are physically located in the Bowie Computer Center.
- c. CEN35 EAD Windows Applications System does not interconnect with any systems outside of the Economic Directorate boundaries. (i.e. systems that share the same System Owner and Authorizing Officials)
- d. The CEN35 EAD Windows Applications System is comprised of three types of applications: census and survey data collection, data processing, and information dissemination.

- e. The applications operate to achieve their intended goals based on the type of application<sup>1</sup>:
  - i. Data collection applications operate in the DMZ to be accessible to the respondent community. Applications limit the access for a respondent to that data that she/he is responsible for providing. Thorough testing is performed prior to releasing applications to production and WebInspect scans are done on a monthly basis.
  - ii. Data processing applications (and subcomponents) are not available to external users. Internal Census Bureau users log on to the data processing applications and perform predetermined tasks as determined in the user requirements.
  - iii. Information dissemination applications are available in the DMZ and provide public access to publicly accessible content through websites designed for presentation of data.
- f. The type of information collected, maintained, use, or disseminated is dependent on the type of application:
  - i. Data collection applications collect Title 13, Title 13 section 9b data, or information that is documented by OMB as being “public content” (i.e. not confidential).
  - ii. Data processing applications utilize Title 13, Title 13 section 9b data, or information that is documented by OMB as being “public content” (i.e. not confidential).
  - iii. Information dissemination applications provide publicly accessible content (i.e. not confidential) to users. In the case when information is not publicly accessible content, valid username and password is required to access the content.
- g. Individuals who have access to information is dependent on the type of application:
  - i. Data collection applications are accessed by respondents (i.e. not federal employees) who can enter data for the entity that they reporting on behalf of. Application administrators who have access to a data collection application are federal employees or contractors employed by the Census Bureau.
  - ii. Data processing applications are accessed by federal employees or contractors employed by the Census Bureau.
  - iii. Information dissemination applications of information that is considered publicly accessible content have a user community that includes anyone with internet access. Information dissemination applications that provide information that is not considered publicly accessible content have a user community that is limited to federal employees, including contractors, who have valid usernames and passwords.

---

<sup>1</sup> All applications are required to meet Census Bureau IT Security requirements which are based on NIST SP 800-53 and NIST SP 800-53a. Additional IT Security requirements are added to the BOC ITSPP based on the DOC ITSPP.

- h. Information retrieval by the user is dependent on the type of application<sup>2</sup>:
  - i. For data collection applications, respondents access their data through a response identifier which identifies the entity or the person reporting. Application administrators retrieve response data based on the response identifier and retrieve user related information based on the userid.
  - ii. For data processing applications, users/analysts retrieve the data based on identifiers that uniquely identify an entity<sup>3</sup>.
  - iii. For data dissemination applications that require user log on, users retrieve the data based on identifiers that uniquely identify the entity.
- i. The exact type of information transmission to and from an application is dependent on the type of application:
  - i. For data collection applications, data transmission leverages TLS 1.2 on the public facing websites. Databases are initialized internally before making the data collection application available to respondents. Encryption is required on all transmissions.
  - ii. For data processing applications, the databases are initialized by automated processes. All applications are available only inside the firewall and encryption is required on all transmissions
  - iii. For data dissemination applications, data transmission leverages TLS 1.2 on the public facing websites. Encryption is required on all transmissions.

---

<sup>2</sup> Systems of Records exist for all projects where the information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The SORNs associated with CEN35 are Commerce/Census – 4, OPM/GOV-5, and COMMERCE DEPT 18 – Employees Personnel Files Not Covered by Other Agencies.

<sup>3</sup> A record may be associated with an individual, business, or government.

**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 (ex. Libraries and Prisons)

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.

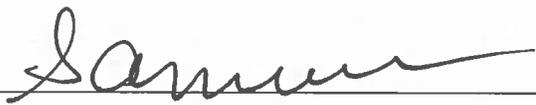
***If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.***

## CERTIFICATION

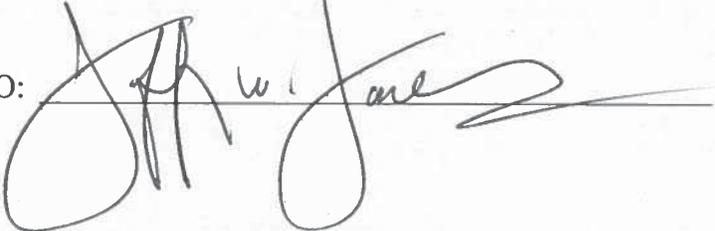
X  I certify the criteria implied by one or more of the questions above **apply** to the CEN35 EAD Windows Applications System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

CEN35 System Owner (SO): Samuel C. Jones

Signature of SO:  Date: 6/24/19

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

Signature of CISO:  Date: 25 Jun 2019

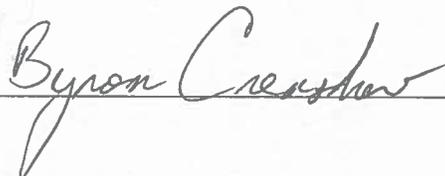
Name of Technical Authorizing Official (AO): Kevin B. Smith

Signature of AO:  Date: 6/26/19

Name of Business Authorizing Official (AO): Nick Orsini

Signature of AO:  Date: 6/26/2019

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BCPO:  Date: 6/26/19