

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



Privacy Threshold Analysis
for the
Enterprise Applications

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/ Enterprise Applications

Unique Project Identifier: 006-000401700

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).

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

The Enterprise Applications system is the functional management framework used to deliver applications to end users of the U.S. Census Bureau network. The Enterprise Applications system contains a variety of systems and applications that maintain or collect personally identifiable information (PII). They are:

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

(b) System location

Enterprise Applications resides at the following locations:

- Bowie, Maryland
- AWS GovCloud is located in Oregon and Ohio

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

Enterprise Applications systems interconnects with infrastructure services at the U.S. Census Bureau. This includes Data Communications for authentication/telecommunication purposes, Network Services for server/storage, and Client Services for laptops and workstations.

In addition, the Enterprise Applications systems interconnect with the following Census Bureau systems:

- Administrative Systems Vol II
- Decennial 2020 Census Infrastructure
- Decennial
- Field
- Demographic Census, Surveys, and Special Processing
- Associate Directorate of Communications (ADCOM)
- Centurion
- Human Resources Applications
- National Processing Center
- Cloud Research Environment
- Lenel
- Economic Census and Surveys and Special Processing
- Commerce Business Systems
- Cloud Services
- Enterprise Tools and Development Services (ETDS)
- Budget Systems
- American Fact Finder - Data Access & Dissemination Systems (AFF-DADS)
- Office of Information Security (OIS) Systems
- Foreign Trade Division Applications

(d) The purpose the system is designed to serve

Enterprise Applications PII/BII is maintained for administrative purposes, statistical and research purposes, and information sharing initiatives,

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

The purpose of the enterprise-level data tracking systems are to ensure data consistency, data integrity, and generate meaningful data information through data management, tracking, and reporting for Census Bureau collections.

The general support systems for Enterprise Applications provide internal data management within the Census Bureau collections. This system allows users to request access to datasets, and

when approved, users are granted access to the datasets within a secure environment provisioned by the system. Census Bureau datasets are for internal use by employees, and are capable of containing protected or administrative information.

The transaction-based systems within Enterprise Applications serve as the primary mechanism for operational control across surveys for data collection. The system can be considered an operational brain that determines operational workflow based on pre-existing protocols.

The relational database management systems store and retrieve data as requested by other software applications. This system provides both a testing, development and production environment for optimum functionality.

The CAES serves as the enterprise-wide analytics platform for surveys and censuses. This system allows statisticians within census and survey projects to perform statistical models using census and survey response data, paradata, administrative records, and many other types of data. The system will receive PII including Identifying Numbers, General Personal Data, and Work-Related Data. The PII is received from other information systems that collect, maintain and disseminate Census and Survey data.

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

The PII/BII maintained for administrative purposes: This IT system maintains first name, last name, address, email address, etc. to ensure that mandatory survey or statistical, information is ready for internal Census use. The information pertains and is in reference to federal employees/contractors conducting the surveys and the public.

The PII/BII maintained for statistical and research purposes: The data maintained by this IT system is collected from other IT systems that collect censuses and surveys (e.g., responses and statuses) and is used to direct data collection efforts. It is also used to inform program areas within the Census Bureau (responsible for survey and census questionnaire mail out) whom to send survey and census forms to. The IT system gathers response data from the data collection modes to send it to the survey and census processing IT systems in a standardized way. This information enables the Census Bureau to fulfill its legal obligation to provide mandated statistics. The information pertains to members of the public.

The PII/BII maintained for information sharing initiatives: This information is collected and shared within the Census Bureau and the Department of Commerce to create datasets for various types of censuses and surveys. This information enables the Census Bureau to fulfill its legal obligation to enhance its information sharing initiatives. The information pertains to members of the public.

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

U.S. Census Bureau government employees and contractors.

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

Authorized users can retrieve information within Enterprise Applications by personal identifiers.

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

Information is transmitted securely via Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS).

(j) Any information sharing conducted by the system

The enterprise-level data tracking system does not share information.

The general support system shares information within the Census Bureau by querying indexed metadata and by sending email to data owners, administrators, and other application users.

The relational database management system does not share information.

The transaction-based system shares demographic survey, Decennial, and Economic Census information within the Census Bureau and with the Department of Commerce, that is used to determine new survey content, support electronic collections, for statistical purposes, and to create datasets for the Census Bureau.

The Concurrent Analysis and Estimation System (CAES) is an environment for use by researchers to make decisions during the data collection phase of a survey or a Census. The CAES system will provide the researcher with any data that they request as input and will output and send decision based data only to other systems. This could include things such as case level intervention codes, a stop work decision, or best time of day to contact respondents. CAES does not provide a mechanism for sharing PII/BII with other systems.

Questionnaire:**1. Status of the Information System****1a. 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 01-2017). *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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

- ☐ Yes. This is a new information system.
- ☐ Yes. This is an existing information system for which an amended contract is needed.
- ☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.
- ☒ No. This is not a new information system.

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.)

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

☒ 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
- ☒ 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.

Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ 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 PIA and the approved SAOP 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 Enterprise Applications 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.

System Owner Name: David J. Peters Office: Application Development & Services Division Chief Phone: (301) 763-9359 Email: david.j.peters@census.gov Signature: <u>DAVID</u> Digitally signed by DAVID PETERS Date signed: <u>PETERS</u> Date: 2021.08.25 16:13:12 -04'00'	Chief Information Security Officer Name: Beau Houser Office: Office of the Chief Information Officer Phone: 301-763-1235 Email: beau.houser@census.gov Signature: <u>BEAU</u> Digitally signed by BEAU HOUSER Date signed: <u>HOUSER</u> Date: 2021.09.02 11:45:25 -04'00'
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763- 7997 Email: byron.crenshaw@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: <u>BYRON</u> Digitally signed by BYRON CRENSHAW Date signed: <u>CRENSHAW</u> Date: 2021.09.30 11:43:21 -04'00'	Agency Authorizing Official Name: Luis J. Cano Office: Chief Information Office Phone: (301) 763-3968 Email: luis.j.cano@census.gov Signature: <u>LUIS CANO</u> Digitally signed by LUIS CANO Date signed: <u> </u> Date: 2021.09.22 16:17:25 -04'00'
Bureau Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763- 7997 Email: byron.crenshaw@census.gov Signature: <u>BYRON</u> Digitally signed by BYRON CRENSHAW Date signed: <u>CRENSHAW</u> Date: 2021.09.30 11:43:39 -04'00'	Business Authorizing Official Name: N/A Office: Phone: Email: Signature: <u> </u> Date signed: <u> </u>