

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



**Privacy Threshold Analysis
for the
CEN05 Field Systems Major Application System**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/ CEN05 Field Systems Major Application System

Unique Project Identifier: 006-000401400

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).

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

The CEN05 Field Systems Major Application System is a major information system managed by the Application Development Services Division (ADSD) in support of the Census Bureau Field Directorate.

(b) System location

The IT system is housed at the Census Bureau's Bowie, MD computer center. There are also components hosted in the Amazon Web Services (AWS) cloud, located in the Northeastern part of the United States.

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

CEN05 interconnects with other IT systems. Desktop and laptop client services are provided by CEN17; server support is provided by CEN16; Oracle 12c database support is provided by CEN18, and; Decennial support is provided by CEN08 TI.

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

The Field Directorate plans, organizes, coordinates, and carries out the Census Bureau's field data collection program for sample surveys, special censuses, the Economic Census, and the Decennial census. The CEN05 IT system maintains Personally Identifiable Information (PII) collected from respondents for these surveys and censuses such as name, address, contact information, race, gender, education, financial information, etc. In addition, Field Representative characteristics are also collected while surveys and census interviews are conducted.

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

Laptops are used to collect survey data in the field. An application assigns cases and monitors interviewing progress. Information systems covered by other CEN plans are used as routing mechanisms to transfer survey data from various survey sources, that includes but are not limited to, computer interviewing, telephone interviewing utilizing Census Bureau computer programs, internet self surveys, and paper surveys to the survey sponsors.

In addition to laptops, the Field Directorate has begun utilizing both tablet and other mobile computing devices to perform Census tests that lead up to the 2020 Decennial Census to collect respondent information using Census Bureau-issued mobile devices.

The Customer Experience Management (CEM) System is a centralized data store from five data sources currently being utilized by the Census Bureau and will deploy an enterprise dashboard for Census Bureau leadership.

This dashboard will provide insights into customer engagement for Census Bureau products & services, and will allow analysts to leverage data across data sources on a holistic Business Intelligence (BI) platform. The system will not only eliminate manual processes, but will:

- 1) Create an opportunity for a better understanding of patterns and trends of customer experiences that can lead to actionable improvement plans, and;
- 2) Establish a framework and foundation for other data integration, BI, and analytics efforts.

CEM will interface/collect information for various sources inside and outside of the Census Bureau and will contain PII data.

The Census Enterprise Data Collection and Processing initiative (CEDCaP) is a suite of IT systems and supporting infrastructure to handle data collection and processing for the nearly 100 surveys and three censuses conducted by the Census Bureau. CEN05 is part of this infrastructure and includes the *Enterprise Censuses and Surveys Enabling platform (ECaSE)* which will provide about half the data collection capabilities for CEDCaP

The ECaSE – ISR (Internet Self-Response) secure Internet data exchange system is a web-based framework for the design, delivery, and execution of surveys, censuses, and other data collection and data exchange efforts over the Internet. The enterprise-level application offers data collection areas the ability to reach a large number of potential respondents online, in a customizable manner to suit their business needs. ECaSE – ISR is developed to support increased demand for online data collections, including the extremely high loads associated with the 2020 Decennial Census.

ECaSE – OCS (Operational Control System) will serve as the standard tool to assign, control, track, and manage listing, survey and census workloads for the field workforce. ECaSE – OCS provides an enterprise application framework for this need, regardless of the interviewer-assisted mode used (phone or in person).

Enumeration is additional functionality given to the ECaSE to support respondents and the overall CEDCaP initiative. For Internet data capture, providing real-time edits, ability to

capture household entries, and multi-access methods across different technologies (e.g., computers, phones, tablets, kiosks).

To establish a cohesive IT system boundary for the purposes of security assessment, the CEN05 IT system is comprised of three major areas: Collections, Business Support Processes, and Backend Processes. Each of these major components employs security control mechanisms that must be individually documented to ensure that the system as a whole is appropriately protected. As such, the system security plan is organized to reflect the implementation of technical controls for each subsystem component.

Application Development and Software Division (ADSD) incorporated a Survey Field Identification Tool (sFIT) to aid in investigating situations where it is suspected that a Field Representative (FR) may be falsifying respondent information. The tool will be used by Contact Center and Regional Office (RO) representatives to indicate FR who are suspected of falsification and to facilitate and document the results of the investigations. The newly developed tool replaced the previous automated system and the paper 11-163 forms. sFIT collects and disseminates PII regarding a survey respondent and the Field Representative who is suspected of falsifying survey data.

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

The CEN05 IT system maintains Personally Identifiable Information (PII) collected from respondents for these surveys and censuses such as name, address, contact information, race, gender, education, financial information, etc. In addition, Field Representative characteristics are also collected while surveys and census interviews are conducted.

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

Authorized Census Bureau employees and/or contractors.

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

There are many external sponsors, but CEN05 does not have direct connections to any of them. Demographics Survey Division (DSD), the Economics Directorate, etc., will give CEN05 the surveys that they have crafted for the external sponsors and the data collected for those surveys is placed into the CEN05 Master Control System (MCS) for the internal system to pick up. It will be the other internal sponsors' responsibility to vet the information, transform it into a format that the external sponsors can ingest and send it off. The sharing of the data should be on those systems with the external connection to the external sponsors. Individual or household records containing PII are retrieved by any number of personal identifiers collected including name, address, contact information, etc..

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

Data collected via CEDCAP and ECaSE is transmitted to the CEN05 IT secure data warehouse. The Data warehouse extracts and provides a view of survey data over time, data collection modes, and data collection operations. It aggregates data and creates canned reports. These reports are made available to stakeholders, approved individuals, and organizations to support optimization and coordination of decennial, current, and special surveys. The reports are developed by a special staff that was established through the Office of the Director to serve as an analytic team with specific, ongoing responsibilities to develop analytic tools (charts and tables). These tools will be used by decennial and current survey field managers toward the goal of continuous improvement in survey operational efficiency. This group will both initiate and respond to issues related to survey performance indicators including cost, data quality, and data collection progress. This database interfaces with systems throughout the Census Bureau that contain PII, Business Identifiable Information (BII), and data collected and/or protected under Title 13 and Title 26.

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): Some added components are in the cloud			

- 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.*

CEN05 collects, maintains, and disseminates audio recordings as part of its support of survey collection activities.

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

X I certify the criteria implied by one or more of the questions above **apply** to the CEN05 Field Systems Major Application 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.

Name of Information System Owner (SO) (All components except ECaSE and its Subsystems):
David J. Peters

Signature of SO:  Date: 8/13/19

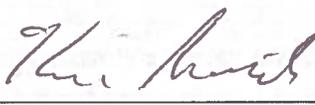
Name of Information System Owner (SO) (ECaSE and its Subsystems): Michael T. Thieme

Signature of SO:  Date: 8/15/19

Name of Deputy Chief Information Security Officer: Jeffery W. Jackson

Signature of DCISO:  Date: 20A062015

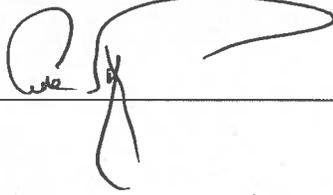
Name of Technical Authorizing Official (TAO): Kevin B. Smith

Signature of TAO:  Date: 8/20/19

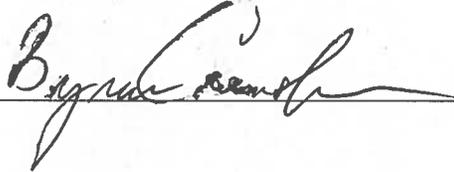
Name of Business Authorizing Official (BAO) (Field): Gregg Bailey

Signature of BAO (Filed):  Date: 8/20/19

Name of Business Authorizing Official (BAO) (ECaSE): Albert Fontenot, Jr

Signature of BAO (ECaSE):  Date: 8/20/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO:  Date: 8/29/19