

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



**Privacy Threshold Analysis
for the
CEN03, Economic Census and Surveys and Special Processing**

U.S. Department of Commerce Privacy Threshold Analysis

CEN03, Economic Census and Surveys and Special Processing

Unique Project Identifier: 006-000400700

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

CEN03 consists of general support systems and major applications to support Economic statistics and survey collection.

(b) System location

All CEN03 components reside on servers located in Bowie Computer Center (BCC).

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

The CEN03 IT system interconnects with internal Census Bureau systems for the purpose of statistical data collection and processing. The CEN03 IT system includes an eCorrespondence project whose goal is to deliver a platform for both incoming and outgoing interactions with customers that can be reused across the Census Bureau by all directorates. It is comprised of a: 1) web application, and 2) PEGA customer relations management (CRM) tool. Each component has a different function, purpose, and interconnection as described below.

Externally, the eCorrespondence portal allows users to have authorized access via the eCorr portal to the Centurion system (CEN15) which stores and manages the survey data. Members of the public accessing Centurion are survey or census respondents. For respondents, the eCorrespondence portal is designed to simplify survey data collection and processing across the enterprise in a cost and time efficient manner.

Internally, the eCorrespondence (eCorr) CRM allows Census Helpdesk Support staff to receive customer inquiries organized into cases and provide resolutions while performing outbound communication based on customer preferences and business rules. The eCorr CRM shares information with the Customer Experience Management (CEM) (CEN05) system about specific cases, which includes CEM customer PII/BII, commitments, events, organizations, contacts, general service requests, data outreach and Frequently Asked Questions (FAQs). Because of the web form component within Pega Customer Relations Management (CRM) system, there is potential internal sharing of encrypted PII, BII or Title 26 if it is included by the respondent within the web form messages.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The Economic Directorate utilizes the IT system for statistical purposes:

The U.S. Census Bureau Economic Programming Directorate is responsible for statistical programs that measure and profile businesses and government organizations in the United States. ECON activities are wide reaching and include: (1) conducting an Economic Census and a Census of Governments every five years; (2) conducting over 50 current surveys taken monthly, quarterly, and annually, including twelve principle economic indicators for the U.S economy; (3) the compilation of administrative records from other government agencies; and (4) facilitating numerous research and technical studies.

The CEN03 IT system has various applications. The applications are designed to accommodate numerous surveys with differing requirements and support all aspects of survey processing. Integrated modules that perform administrative functions allow users to modify the application to meet survey requirements. The surveys process both Title 13 and Title 26 data excluding the construction monthly surveys, which are project based. These applications provide data entry, editing, imputation, data review and correction, estimation and variance estimation. Also, the Census Bureau's master list of businesses called the Business Register (BR). The primary mission of the BR is to provide a complete, unduplicated universe of statistical units that can be used to construct business survey sampling frames and provide a basis for Economic Census enumeration.

The Economic Directorate utilizes the IT system for administrative matters:

The Economic Directorate survey areas use data to create mailing lists of registered businesses. This mailing list designates which individuals receive an authorization code in the mail so that they can submit data for economic-related surveys that are housed in Centurion, which is accessed via the eCorrespondence portal. Use of IRS data allows the ECON directorate to identify the proper individuals who will submit data on behalf of their companies. The eCorrespondence portal collects only enough data to confirm the identity of the individual and create an account for self-service, survey support, and survey collection functionality.

The Economic and Communications Directorate utilize the IT system to improve Federal services online:

The Economic Directorate utilizes the eCorrespondence web application sub-component for approved Census Bureau customers to access survey data. This application performs several survey-related transactions that improve services. For example, users can request a time extension for completing surveys, delegating a survey to another individual, or accessing the Centurion survey data collection system through single sign-on.

For the Communications Directorate, the purpose of the system is to provide the Census Bureau the capability to capture, route, track and respond to every visitor-initiated query that comes through the Census.gov channels. It also allows the Census Bureau to manage its Frequently Asked Questions (FAQ) database and allows website visitors to view and subscribe to receive email notifications when FAQs are updated and can provide real-time customer support by allowing web visitors to submit inquiries via a chat interface.

The Economic Directorate utilizes the IT system for customer satisfaction and online services:

For eCorrespondence, there are two main transaction types in the eCorrespondence system. The first is a respondent self-help transaction. A business respondent logs in and authenticates via a component in the CEN01 security boundary to access the eCorrespondence web application and performs one or more survey-related transactions. This includes requesting delegation of a survey to another individual or accessing the Centurion survey data collection system through single sign-on, etc.

The second type of transaction is a support request. These transactions are managed by the Pega CRM tool. A business respondent can request direct support for a specific survey via secure messaging. Similarly, an anonymous user can submit a message for general support (e.g., for help registering or logging into the website). Support representatives view the submitted secure messages as cases and respond to customers providing interactive support. Only internal Census Bureau staff with a need-to-know may access or view these records.

The goal of the eCorrespondence project is to deliver a platform for both incoming and outgoing interactions with customers that can be reused across the Census Bureau by all directorates. Internally, eCorrespondence Pega will allow Census Helpdesk support staff to receive customer inquiries organized into cases and provide resolutions while performing outbound communication based on customer preferences and business rules. PII/BII is collected to support user account management for survey related transactions. Additionally, the system is also used to document data dissemination activities and to capture interactions with data users. It is also used to track all Census Bureau partnership activities and activities between the Census Bureau and outside organizations.

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

Information (whether personally identifiable information (PII) or business identifiable information (BII)) collected by this IT system are personal names, personal addresses, personal contact information (telephone numbers, email address), business information, occupation, tax information, account information etc. The information is retrieved by PII/BII by Census Bureau staff who have a business need to know. Only Census Bureau employees and their agents with Special Sworn Status can access data under Title 13 U.S.C. Title 13, U.S.C. Section 23 (c) permits the Census Bureau to provide Special Sworn Status to individuals who must access Census Bureau data to assist the Census Bureau in carrying out the work of its title.

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

The data is transferred through Electronic Data Transfer (EDT) through the use of: 1) automated rule-based routing and 2) Managed File Transfer (MFT) software components of the system. The EDT system MFT utilizes data integrity checking (hashing) of file content, detection of transfer errors, and recovery from points of failure. The EDT system MFT establishes a secure connection and hashes each packet of data using SHS algorithms. The result(s) of the hashes are transmitted with each

packet of data. Encryption is done in-stream, packet by packet, and transmitted to the destination EDT server. Encryption is implemented for data in transit such as SSL/HTTPS to ensure secure transmission of data and web services utilize encrypted security tokens during transmission of data to prevent access to data outside of an authenticated and valid session and [also implemented for data at rest in the databases](#). Completed data transfers utilize automated rule-based routing (scripting) at destination endpoints for secondary (PIK) processing and quality assurance (QA) against control files.

The eCorrespondence distributes unique, one-time use Authentication Codes mailed to respondents for each survey the respondent participates. When registering or adding a survey to an existing eCorrespondence account, Authentication Codes are verified against data provided by Centurion and eCorrespondence associates a survey to a user account in the eCorrespondence database and updates the authentication code bank that the authentication code has been used. Pega CRM provides transactional updates to the eCorr database and queries authentication code status to ensure the code is valid for a specific respondent and associated survey.

(g) Any information sharing conducted by the system

The information in this IT system is shared within the Census Bureau and with other federal agencies such as the Bureau of Justice Statistics, National Center for Education Statistics, Bureau of Transportation Statistics, the Federal Reserve Board, National Science Foundation, U.S. Environmental Protection Agency, Agency for Healthcare Research and Quality, Department of Energy, and the U.S. Department of Housing and Urban Development. In addition, information is shared to the private sector via the Management and Organizational Practices Survey (MOPS) data that is given to the survey sponsors (at Stanford, Massachusetts Institute of Technology, London School of Economics, and the University of Toronto).

Because of the web form component within Pega Customer Relations Management (CRM) system, there is potential internal sharing of encrypted PII, BII or Title 26 if it is included by the respondent within the web form messages. Internally, eCorrespondence (eCorr) CRM allows Census Helpdesk Support staff to receive customer inquiries organized into cases and provide resolutions while performing outbound communication based on customer preferences and business rules.

The eCorr CRM shares information with the Customer Experience Management (CEM) (CEN05) IT system about specific cases, which includes CEM customer PII/BII, commitments, events, organizations, contacts, general service requests, data outreach and Frequently Asked Questions (FAQs).

The data shares include a one way exchange of data from the Micro Analytical Database (MADb) (CEN03) to the Unified Tracking System UTS (CEN05) to support UTS analysis and reporting of survey response rate information for the Company Organization Survey and the Annual Survey of Manufactories (COS/ASM). This data share is internal to survey managers and researchers.

ECON survey paradata is also internally shared with the Master Control System (MCS) (CEN05) and Centurion (CEN15). MCS tracks inputs of survey paradata for data collection and capture and produces outputs of the input data for retrieval by ECON surveys.

ECON also shares read-only public use tabulated data from the Rental Housing Finance Survey (RHFS) with Demographic Statistical Methods Division (DSMD) (CEN11) to create custom tables of organized data access and visualization of RHFS survey data.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

13 U.S.C., Chapter 5, 6, 8(b), 131, 161, 182, 193, and OMB Circular A-133.

For the e-correspondence web application and PEGA CRM system, the following authorities apply: 5 U.S.C. 301 and 44 U.S.C. Section 3101

(i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

The Federal Information Processing Standard (FIPS) 199 security impact category for this IT system is Moderate.

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.*
- 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.)

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 about: (Check all that apply.)

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
- 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.

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 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 CEN03 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 CEN03 System Owner (SO): Sumit Khaneja

Signature of SO: **SUMIT KHANEJA** Digitally signed by SUMIT KHANEJA
Date: 2020.08.05 21:40:14 -04'00' Date: _____

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

Signature of CISO: **BEAU HOUSER** Digitally signed by BEAU HOUSER
Date: 2020.08.11 14:30:57 -04'00' Date: _____

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

Signature of AO: **KEVIN SMITH** Digitally signed by KEVIN SMITH
Date: 2020.08.13 12:43:43 -04'00' Date: _____

Name of Business Authorizing Official (AO): Nick Orsini

Signature of AO: **NICK ORSINI** Digitally signed by NICK ORSINI
Date: 2020.08.06 14:28:28 -04'00' Date: _____

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: **DAVID DONOVAN** Digitally signed by DAVID DONOVAN
Date: 2020.08.14 09:44:10 -04'00' Date: _____