Version Number: 01-2020

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

Privacy Threshold Analysis
for the
CEN04 Commerce Business Systems (CBS)

U.S. Department of Commerce Privacy Threshold Analysis

CEN04 Commerce Business Systems (CBS)

Unique Project Identifier: 006-000401500

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 Commerce Business System is a major application that provides financial management and accounting capabilities for Budget/Funds Management, Accounts Payable, Accounts Receivable, Reimbursable Agreements, Cost Accumulation, General Ledger, and Financial Reporting.

(b) System location

CBS is hosted at the U.S. Census Bureau Bowie Computer Center.

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

CEN04 CBS interconnects with internal Census Bureau IT systems to leverage enterprise services (CEN01 Data Communications, CEN16 Network Services) and inherit security controls provided by the Enterprise Common Control Providers (ECCP). CEN04 CBS also interconnects with CEN05 Field, CEN06 National Processing Center, CEN17 Client Services, CEN18 Census Data Lake, CEN20 Budget Division, CEN21 Human Resources Applications, and CEN31 Administrative to share information. CEN04 has interconnections with DOC-wide systems such as CSTARS (Acquisitions System for DOC), Financial Management Service (FMS)/Bureau of the Public Debt, Commerce Learning Center (CLC) and with government-wide systems such as E2 – Government Travel Systems and SmartPay3 (credit card systems at Citibank).

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

The purpose of CEN04 CBS is for administrative matters.
The statements below cover all personnel data within CBS including the information for Census Employees, Census Contractors including Foreign Nationals, and Special Sworn individuals. No personal data regarding the general public is in CBS. For administrative matters

- Social security number (SSN) and/or taxpayer identification number (TIN) identify an individual and "sole proprietor" business where the SSN is used as the identifier or the TIN, whichever is appropriate. A Taxpayer Identification Number (TIN) is a nine-digit number, which is either an Employer Identification Number (EIN) assigned by the Internal Revenue Service (IRS) or a Social Security Number (SSN) assigned by the Social Security Administration (SSA). Agencies are required to collect TINs [Debt Collection Improvement Act, 31 U.S.C. 7701(c)] and to include the TIN in vouchers submitted for payment [31 U.S.C. 3325 (d)].
- Name, address, and contact information are required to identify and to contact an individual or business. This identifying information is also part of the criteria to identify a vendor to determine eligibility for registration in the General Services Administration (GSA) managed government-wide System for Award Management (SAM.GOV), which replaced the prior Central Contractor Registration (CCR) system.
- Identifying information is needed to identify individuals who require access to secure application code content on the CBS Support Center (CSC) Portal as part of the user account registration process.
- Identifying information is needed to identify individuals who require access to applications as part of the user account registration process.
- Identifying information is used to track transactions and activity performed using the applications.
- Date and place of birth and mother's maiden name validates the identity of an individual.
- Bank routing number and individual bank account or electronic funds transfer (EFT) number identify the individual or business and process financial transactions, such as payments.

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

CBS consists of the Core Financial Systems developed by the Department of Commerce and Administrative systems (called Feeders) developed by Census. The applications are written in a mix of Oracle Forms, Oracle Reports, Oracle BI Publisher and Java. They are deployed on Webservers and connect to Oracle databases stored within the BCC in Bowie, MD.

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

a. Social security number (SSN) and/or taxpayer identification number (TIN) identify an individual and "sole proprietor" business where the SSN is used as the identifier or the TIN, whichever is appropriate. A Taxpayer Identification Number (TIN) is a nine-digit number, which is either an Employer Identification Number (EIN) assigned by the Internal Revenue Service (IRS) or a Social Security Number (SSN) assigned by the Social Security Administration (SSA). Agencies are required to collect TINs [Debt Collection Improvement Act, 31 U.S.C. 7701(c)] and to include the TIN in vouchers submitted for payment [31 U.S.C. 3325 (d)].

b. Name, address and contact information are required to identify and to contact an individual or business. This identifying information is also part of the criteria to identify a vendor to determine eligibility for registration in the General Services Administration (GSA) managed government-wide System for Award Management (SAM.GOV), which replaced the prior Central Contractor Registration (CCR) system.

i. Identifying information is needed to identify individuals who require access to secure application code content on the CBS Support Center (CSC) Portal as part of the user account registration process.
ii. Identifying information is needed to identify individuals who require access to applications as part of the user account registration process.
iii. Identifying information is used to track transactions and activity performed using the applications.

c. Date and place of birth and mother's maiden name validates the identity of an individual.

d. Bank routing number and individual bank account or electronic funds transfer (EFT) number identify the individual or business and process financial transactions, such as payments.

(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

The users utilize the CBS menu system, through a browser, to access the pieces of the application that they are authorized to access. The application pulls data from the Oracle databases and displays it to the users.

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

Information between the user and the F5 load balancers is encrypted using https.

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.*

__X_ 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.

_X__ 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.

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

_X___ 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.)*

__X__ 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."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X__ DOC employees
_X_ 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.

_X__ 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?

_X__ 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.

_X__ 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 the CEN04 Commerce Business Systems (CBS) 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: Chief, Application Development and Services Division Phone: 301-763-9359 Email: david.j.peters@census.gov Signature: DAVID PETERS Digitally signed by DAVID PETERS Date: 2021.01.28 08:06:49 -05'00' Date signed:	**Chief Information Security Officer** Name: Beau Houser Office: Office of Information Security Phone: (301) 763-1235 Email: beau.houser@census.gov Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2021.02.02 09:13:57 -05'00' Date signed:
Technical Authorizing Official, Acting Name: Gregg D. Bailey Office: Office of the CIO Phone: (301) 763-0989 Email: Gregg.d.bailey@census.gov Signature: GREGG BAILEY Digitally signed by GREGG BAILEY Date: 2021.02.04 12:21:48 -05'00' Date signed:	**Business Authorizing Official** Name: Gregg D. Bailey Office: Office of the CIO Phone: (301) 763-0989 Email: Gregg.d.bailey@census.gov Signature: GREGG BAILEY Digitally signed by GREGG BAILEY Date: 2021.02.12 10:43:05 -05'00' Date signed:
Census Bureau Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763-7997 Email: byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2021.03.02 14:59:53 -05'00' Date signed:	**Privacy Act Officer** Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763-7997 Email: byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2021.03.02 15:00:12 -05'00' Date signed: