Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Office of the Chief Information Officer (OCIO)
Commerce Business Systems (CBS)

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau
Office of the Chief Information Officer (OCIO) Applications Development and Services Division (ADSD)
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: *Provide a brief description of the information system.*

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).

OCIO ADSD Commerce Business Systems (CBS) (known as CBS going forth) is the financial system of record for the Census Bureau. The OCIO CBS 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. CBS consists of the Core Financial Systems (CFS) computer programs developed by the DOC and Administrative IT systems (called Feeders) developed by Census. CBS collects SSN and other identifying information for required administrative purposes and records management.

CBS is made up of Department of Commerce (DOC) developed programing and programing specific to Census Bureau needs. The CFS program is a central component of CBS and provides the financial management and accounting capabilities to support Census Bureau financial operations.

The Census developed portions of CBS are tested, supported and managed by the Census Applications Development and Services Division (ADSD), while CFS system testing and software development is performed by the DOC CBS Support Center (CSC) with additional operational testing and verification by ADSD and Census Finance Division within the Census environment.

Address the following elements:

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

The CBS 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)

CBS interconnects with internal Census Bureau IT systems to leverage enterprise services (Office of the Chief Information Officer (OCIO) Telecommunications Office (TCO) Data Communications, Office of the Chief Information Officer (OCIO) Computer Services Division (CSvD) Network Services) and inherit security controls provided by the Enterprise Common Control Providers (ECCP). OCIO CBS also interconnects with Office of the Chief Information Officer (OCIO) Field, Associate Director for Field Operations (ADFO) National Processing Center (NPC), Office of the Chief Information Officer (OCIO) Client Support Division (CSD) Client Services, Office of the Chief Information Officer (OCIO) Enterprise Applications Census Data Lake, Office of the Chief Financial Officer (OCFO) Budget Division (BUD), Office of the Chief Information Officer (OCIO) Human Resources Applications, and Office of the Chief Information Officer (OCIO) Application Development & Services Division (ADSD) COTS Integration Branch (CIB) Administrative systems to share information. OCIO CBS 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 OCIO CBS 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.

CBS consists of the CFS computer programs developed by the DOC and Administrative IT 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.

e) A general description of the type of information collected, maintained, used, or disseminated by the system

a. Social security number (SSN) and/or taxpayer identification number (TIN) is used to identify an individual and/or a "sole proprietor" business where the SSN is used as the identifier or the TIN, whichever is appropriate. 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 other contact information are required to identify and to contact an individual or business. This identifying information is also apart 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.

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.

f) Identify individuals who have access to information on the system

U.S. Census Bureau government employees and contractors

g) How information in the system is retrieved by the user

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

h) How information is transmitted to and from the system

Transmitted information between the users and the CBS application is encrypted using HTTPS. There is no public access to CBS.

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. *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. *(Check all that apply.)*

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.

__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?

_X__ 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. Financial transactions and data exchanged with payroll systems are linked to Social Security Number.
Provide the legal authority which permits the collection of SSNs, including truncated form. Social security number (SSN) and/or taxpayer identification number (TIN) is used to identify an individual and/or a "sole proprietor" business where the SSN is used as the identifier or the TIN, whichever is appropriate. 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)].

___ 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 SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X___The criteria implied by one or more of the questions above **apply** to the Office of the Chief Information Officer (OCIO) Commerce Business Systems (CBS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the Office of the Chief Information Officer (OCIO) Commerce Business Systems (CBS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Gregg D. Bailey Office: Office of the Chief Information Officer System Owner: OCIO Directorate Phone: 301-763-0989 Email: gregg.d.bailey@census.gov Signature: GREGG BAILEY Digitally signed by GREGG BAILEY Date: 2022.06.15 16:53:10 -04'00' 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: 2022.05.27 12:51:43 -04'00' Date signed:
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: byron.crenshaw@census.gov Signature: DONNA NEAL Digitally signed by DONNA NEAL Date: 2022.06.22 10:30:57 -04'00' Date signed:	**Agency Authorizing Official** Name: Luis J. Cano Office: Office of the Chief Information Officer Phone: (301) 763-3968 Email: luis.j.cano@census.gov Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2022.06.15 14:24:44 -04'00' Date signed:
Census Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: byron.crenshaw@census.gov Signature: DONNA NEAL Digitally signed by DONNA NEAL Date: 2022.06.22 10:31:31 -04'00' Date signed:	