

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



**Privacy Threshold Analysis
for the
CEN20 Budget Division Applications**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau CEN20 Budget Division Applications

Unique Project Identifier: 006-000403600

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*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

The CEN20 BUDGET Division Applications reside at the Census Bowie Computer Center. The Consolidated Budget and Reporting Application (COBRA) is the Census Bureau's budgetary system of record to support budget execution and budget formulation as described in OMB Circular A-11. The only Personally Identifiable Information (PII) stored in COBRA is data about U.S. Census Bureau employees. Census Bureau administrative offices create directorate and division-level project cost estimates, from the ground up, based on salary costs and non-salary costs. To build the salary costs, the administrative offices map which employees work on each project and the proportion of time they will spend on each project during a fiscal year to create a position listing (PL). The position listing is updated using personnel data from the CEN04 Commerce Business System (CBS) and merged with project data from the previous

operating plan or Budget Planning Documents (BPDs). This module contains PII including employee name, job series, grade, and per annum salary, however there is no Social Security Numbers collected. Access to COBRA is limited to those with valid network accounts; access to specific forms and reports in COBRA is controlled through permissions/roles. The user-name (James Bond) and date stamp of users accessing COBRA is logged. The Federal Information Processing Standard (FIPS) 199 security impact category for the COBRA application is Low. The Budget Division within the U.S Census Bureau manages, formulates, and executes the annual budget allocated by the U.S. Congress. The Division utilizes a combination of the Oracle EPM suite and custom .NET applications to manage budget information. Stakeholders, internal and external to the Budget Division (BUD), consume financial reports generated with data from different sources including budget data. The reports generated currently do not meet the standards of an efficient reporting methodology. Instead of having integrated reports, users must run multiple reports from different data sources. BUD assessed alternatives for generating advanced financial reports and decided to implement an Integrated Financial Reporting solution leveraging SAS Enterprise Business Intelligence (SAS BI).

FIAT is a SAS Business Intelligence/Oracle Data Warehousing solution FIAT provides users with a variety of prebuilt static and dynamic reports and dashboards. Dashboards enable users to monitor Key Performance Indicators that convey how things are performing at any point of time. OLAP cubes (On line analytical processing) cubes can be viewed as a pre-summarized multidimensional format data to improve query processing. The Federal Information Processing Standard (FIPS) 199 security impact category for the FIAT application is Medium. The IT system is housed at the Census Bureau's Bowie, MD computer center.

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.*

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.*

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 CEN20 Budget Division 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.

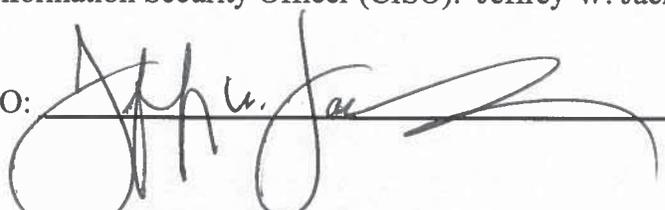
Name of System Owner (SO): James Simpson
JAMES
SIMPSON

Digitally signed by
JAMES SIMPSON
Date: 2019.07.03
13:14:30 -04'00'

Signature of SO: _____ Date: 07/03/2019

Name of Chief Information Security Officer (CISO): Jeffrey W. Jackson, Acting

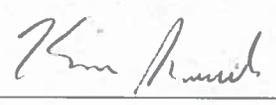
Signature of CISO: _____



Date: 7/5/2019

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

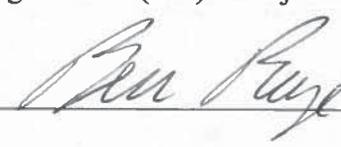
Signature of AO: _____



Date: 7/3/19

Name of Authorizing Official (AO): Benjamin Page

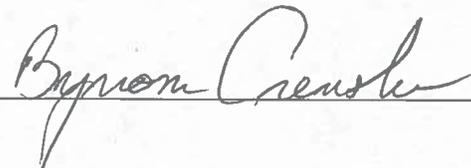
Signature of AO: _____



Date: 7/3/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: _____



Date: 7/30/19