Version Number: 01-2015

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

Privacy Impact Assessment
for the
CEN20 Budget Division Applications

Reviewed by: Byron Crenshaw, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2019.09.26 12:44:59 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau CEN20 Budget Division Applications

Unique Project Identifier: 006-000403600

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in 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 COBRA application is Medium.

(b) a description of a typical transaction conducted on the system;

COBRA: Users enter budget planning information into COBRA as the first step to, ultimately, establishing budgetary resources in the core financial system

Currently, the monthly Variance Reports are generated by the Commerce Business System (CBS) financial management system. A budget analyst in the Budget Systems staff, or SAB, will download the reports at month end and upload them to the BUD intranet site on SharePoint. Divisions outside of BUD can view the reports.

The FIAT system will extract data from CBS on a nightly basis. Users will be granted permission to view both selected standard web reports and cube reports. The cube reports allow ad hoc analysis by formatting reports by dragging fields to and from the report layout. If a user creates a report that they would like to keep for the future, preferences may be stored by the user and can be run at any point in time. FIAT will improve the accessibility, accuracy and frequency of the retrieval of CBS data.

(c) any information sharing conducted by the system; and

Data from COBRA is used as input into the core financial system to formally establish budgetary resources. The core financial system is named CBS (Commerce Business System). There is an Interconnection Security Agreement between these two IT systems. FIAT receives data from CEN04 - Commerce Business Systems (CBS). The CBS security plan provides details to the technical controls where data is protected by firewalls located on the Census Bureau Local Area Network (LAN).

The Decennial Budget Integration Tool (DBiT) owned and operated by the Decennial Census Management Division (DCMD) in the CEN08 Decennial IT security plan supports the DCMD Budget Management staff to perform ongoing cost estimation, budgeting, planning, and execution management functions. The Consolidated Budget Reporting Application (COBRA) is the Census Bureau's budget planning system of record for current and future year allocations owned and operated by the Budget Division (BUD). COBRA requires the use of Budget information for the Budget Planning (BP) and Operating Plan (OP) in order to establish budget constraints in the core financial system (CBS). The BPD and OP parts of COBRA needs employee data from DBiT for its Position Listings. There is a bidirectional Interconnection Security Agreement between these two IT systems.

COBRA and FIAT receive user authentication information from the CEN01 communications network.

(d) a citation of the legal authority to collect PII and/or BII;

31 U.S.C. 66a, 492;
44 U.S.C. 3101, 3309
5 U.S.C 301

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

The high water mark for the CEN20 system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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):					

__X__ This is an existing information system without changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Federal budget formulation and budget execution.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

COBRA:
For COBRA, information about employees is needed to ensure a complete and comprehensive assessment of salary costs are captured. In addition, employee information is needed to ensure all necessary positions, staff, and vacancies are accounted for. Employee-level salary information is combined to support the budget formulation and budget execution process described in OMB Circular A-11.

The PII/BII identified in section 2.1 for the COBRA system is in reference to Federal employees only.

FIAT:
The purpose of FIAT is to deliver an Integrated Financial Reporting solution to enhance analytical reporting capabilities, including, but not limited to: developing an integrated reporting infrastructure, building reporting dashboards, enabling ad hoc and management reporting, integrating multiple identified data sources, and dupporting a new Integrated Financial Reporting platform.

The PII/BII identified in section 2.1 for the FIAT system is in reference to Federal employees and contractors. Detail level PII data is needed to create aggregate and summary level reports for analysis. However, no PII/BII for any Federal employee/contractor, member of the public, foreign national, or visitor will be discernable within any of the reports created within the FIAT system.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: CEN04 CBS CEN08 Decennial (DBIT) CEN01 Data Communications The CEN20 IT system uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.census.gov/about/policies/privacy/privacy-policy.html	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Personal data in COBRA and FIAT are copied from the Census CBS Core Financial System.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Personal data in COBRA and FIAT are copied from the Census CBS Core Financial System.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Personal data in COBRA and FIAT are copied from the Census CBS Core Financial System.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition, audit logs are in place and assessed per NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ____ 7/5/2018 _____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-1.html COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1, 3.2, 4.1, 4.2, 4.3
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Data elements are not directly identifiable alone but may indirectly identify individuals
X	Quantity of PII	Provide explanation: Although a serious or substantial number of individuals would be affected by loss, theft, or compromise, the PII collected and maintained is non-sensitive which is unlikely to result in harm to individuals.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, have little relevance outside the context.
X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, or the PII itself is unlikely to result in harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.
X	Access to and Location of PII	Provide explanation: Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed by organization- owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)).
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.