Version Number: 01-2015

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

Privacy Impact Assessment
for
CEN04 Commerce Business Systems (CBS)

Reviewed by: Byron A. Crenshaw; Chief Privacy Officer, Acting

☒ 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 12:32:53 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
CEN04 Commerce Business Systems (CBS)

Unique Project Identifier: 006-000401500

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

Functional and administrative systems provide additional operational capabilities, which augment the Census Bureau's accounting processes. These functional/administrative systems in CBS include Purchase Card, Travel, Training, and Labor Cost Distribution. Other functional/administrative systems provide information to or receive information from the Core Financial System (CFS) via various interfaces. CFS is the central component of CBS, which provides financial management and accounting capabilities through the following modules/applications: Budget/Funds Management; Accounts Payable; Accounts Receivable; Reimbursable Agreements; Cost Accumulation; General Ledger; and Labor Cost Distribution.

Data within CBS includes personal information about Census Employees, Census Contractors including Foreign Nationals, and Special Sworn individuals including Foreign Nationals. No personal data regarding the general public is in CBS.

Data types in this system include: Budget formulation, budget execution, central personnel management, entitlement event Information, facilities management, security management, financial asset and liability management, financial reporting, accounting, payments, collections and receivables, benefits management, Human Resources development, system maintenance, information management, and personal identity and authentication management information.

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

Commerce Purchase Card System (CPCS) is used to document, reconcile, approve and process all Census Bureau credit card charges made by CBS users/credit card holders. CPCS includes assistance from Acquisitions, Finance and Budget and National Oceanic Atmospheric Association/Bank. For example, when a Department of Commerce employee is traveling using a government issued travel card the CPCS tracks and approves credit card transactions.

Education and Training Management Information System (ETMIS+) is used to track, maintain, schedule, and reserve funding for various training courses utilized both internally and externally from the Census Bureau. Census employees utilize this system to get approved for training as well as keep track of class rosters etc.

Overtime Authorization Request Application (OTCD81) is an overtime tracking system that provides options to capture and store employee overtime data.

(c) any information sharing conducted by the system

CEN04 CBS shares administrative information with the following internal Census systems:

CEN05 Field,
CEN06 Nation Processing Center
CEN10 Mobile Enterprise Development Environment
CEN17 Client Services

CBS shares administrative information with the following External systems:

Department of Commerce - Accounting, Payment, and PII data.
Financial Management Service (FMS)/Bureau of the Public Debt - Treasury payment services.
DOC ETS2 Travel Shared Services – Travel management, payments, and PII data for travel.

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

COMMERCE/DEPT-2, Accounts Receivable
COMMERCE/DEPT-17, Records of Cash Receipts
COMMERCE/DEPT-22, Small Purchase Records

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

The Federal Information Processing Standard (FIPS) 199 security impact category for the 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	X	i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): New travel management shared service added by Department of Commerce.					

__X__ This is an existing information system in which changes do not 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*	X	e. File/Case ID		i. Credit Card	X
b. Taxpayer ID	X	f. Driver's License		j. Financial Account	X
c. Employer ID	X	g. Passport		k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Financial transactions and data exchanged with payroll systems are linked to Social Security Number.					

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

Other (specify):

	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	
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):			

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).

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

For administrative matters

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.

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	X
DOC bureaus	X	X	X
Federal agencies	X	X	
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. CEN04 receives information from CEN20 Budget Division, CEN21 Human Resources Division, CEN31 Administrative Systems. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:

	CEN04 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. Census 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: http://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: CBS does not obtain the information from the individual; HR provides the information.

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: The information is payroll data. Per 5 U.S.C. 301 a department head may prescribe the regulations for the government of his department including the conduct of its

		employees and performance of its business, records, & property & individuals do not have opportunity to consent to the uses of the PII that are collected for the purposes stated by the applicable SORNs.

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Human Resources application or via a Privacy Act Request as per the Privacy Act and as identified in applicable SORN.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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

X	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 additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically 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): 7/11/2018 ☐ 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.

Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII 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 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

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 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. Census also deploys a DLP 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-2, Accounts Receivable COMMERCE/DEPT-17, Records of Cash Receipts COMMERCE/DEPT-22, Small Purchase Records
	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: Records Control Schedule 1: Administration and Management Records Control Schedule 2: Financial Management
	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: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. GRS 6, item 1 authorizes the disposal of the equivalent paper copies six years and three months after the period covered by the account, EXCEPT: Accounts and supporting documents pertaining to American Indians are not authorized for disposal. Such records must be retained indefinitely since they may be needed in litigation involving the Government's role as trustee of property held by the Government and managed for the benefit of American Indians.

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

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	
Other (specify): When servers are decommissioned, CEN16 standard procedures are used to sanitize data and / or shred as required by Census procedures.			

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.

	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.
X	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: PII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
X	Quantity of PII	Provide explanation: The collection is for all Department of Commerce employees and contractors, therefore, a substantial number of individuals would be affected if there was loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: PII in this IT system is collected under the authority of Title 5.
X	Access to and Location of PII	The PII is located on computers (including laptops) and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know including the Census Bureau geographic program area, regional offices, and survey program offices, etc. Access is only allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities.
	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.