Version Number: 01-2019

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

Privacy Impact Assessment
for the
ASSOCIATE DIRECTOR FOR COMMUNICATIONS (ADCOM)

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

Jennifer Goode 02/16/2021

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/Associate Director for Communications (ADCOM)

Unique Project Identifier: TBD

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. Please answer each question (a) through (i) separately.

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

Associate Director for Communications (ADCOM)/CEN37 is a general support system that is comprised of three major components that supports the communication services of the U.S. Census Bureau including content direction, content management, creative design and branding, social media management, customer engagement/experience, stakeholder engagement and relations, advertising and promotions. The three major components are:

1) The Content Management System (CMS) within ADCOM/CEN37 provides Software-as-a-Service (SaaS) to host means to facilitate the secure transfer/store/processing of all data. CMS offers clients with a managed web application content solution, running in the FedRAMP validated Amazon Web Services (AWS) cloud computing infrastructure. The following systems/applications components fall within the SaaS boundary of CEN37 – ADCOM:
    - Adobe Experience Managed Manager Services (AEMMS)
    - Adobe Managed Services (AMS).

2) The Data Visualization System (DVS) within ADCOM/CEN37 provides a Platform-as-a-Service (PaaS) to host cloud computing services that provide a platform to allow customers to develop, run, and manage Tableau web applications without the complexity of building and maintaining the infrastructure. Tableau is software application for data visualization that collects PII. DVS offers clients data visualizations publishing for external audiences in Census.gov using publicly available data. Data visualization creators create connections between public data providers and Tableau Desktop and retrieve data files.

    DVS also retrieves data from the external data providers on a scheduled basis and stages the data in a specified location on a server in an isolated DMZ environment. A load job on the internal side retrieves the data files, performs any necessary transformations, and load the raw data (referred to as "Tier 1").

    Lastly, DVS provides clients a solution that employs the 2020 Census TI AirWatch instance to manage field mobile phones, known as Mobile CRM. These users access the application via the Pega Mobile app, deployed to cellular phones using a Mobile Device Manager (MDM). An organization within TI called dDaaS manages AirWatch and, by extension, all

field mobile phones. The CRM team provides a data file for deployment. The following systems/applications components fall within the PaaS boundary of CEN37 – ADCOM:

- Tableau Web Application Server (Formerly Tableau Server)
- Repository Servers (Formerly Customer Experience Manager (CEM))
- Tableau External (Formerly Public Virtualization Platform (PVP))
- Pega Mobile Customer Relationship Manager (CRM)*
- Accenture Insight Platform (AIP)

**Pega Mobile Customer Relationship Manager (CRM) solution manages field mobile phones and is currently the only independent system component within ADCOM/CEN37 that is co-owned with ECON/CEN03 via an established Service Level Agreement (SLA). Mobile CRM user's access the application via the Pega Mobile app deployed to their phones using Mobile Device Management. CEN37 CRM only pulls metrics from CEN03 CRM and does not collect or maintain PII.*

3) Digital Marketing Applications (DMA) within ADCOM/CEN37 are cloud-based, browser accessed, non-Census Bureau-hosted third-party provided, licensed and contracted applications utilized for marketing purposes. ADCOM/CEN37 have a number of Memorandums of Understanding (MOUs) that ensure that full responsibility for managing compliance externally is enforced. This partnership has afforded ADCOM/CEN37 to have approximately fourteen (14) MOUs currently in place.

   - Adobe Target
   - Sprinklr
   - Facebook Leads Generation (Collects PII)
   - StoryPorts
   - Ziflow
   - Campaign Management Platform (CMP – Team Y&R)
   - Federalist
   - Airtable
   - Adobe Analytics
   - Cision
   - Quorum
   - CalendarWiz
   - QuickFacts
   - Solar

(b) System location

ADCOM/CEN37 components predominately reside on the Amazon Web Services (AWS) GovCloud environment. The physical headquarters is located in Seattle, Washington. The production environment for AEMMS is located in the AWS US GovCloud West region. All ADCOM/CEN37 data backups are performed in the AWS Cloud.

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

The services/components in CEN37 are standalone and span over multiple servers, and the physical environment is owned and managed by a third-party vendor at offsite facilities located in the United States. Some cloud services may be logically isolated and designed to allow U.S. government agencies and contractors to move more sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. In addition, the encryption keys are maintained by the Census Bureau. The cloud provider will not have access to the encryption keys

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

CEN37 cloud services is a comprehensive digital communications management solution designed for the public sector. Through multiple platforms on CEN37, Census Bureau staff is able to:

- Manage multi-channel digital communications and maintain continuous contact with members of the public
- Develop visually appealing communications and distribute them across multiple digital channels including email, phone, text messages, and social media lists
- Manage and send messages to these lists; streamline communications, reach more people, and meet the government's mission-critical objectives

The services/components in CEN37 allow the Census Bureau to deliver critical notices to members of the public, enhancing service delivery and enables the creation of virtual communities for collaborating on shared objectives. Access is controlled by registration and is by invite-only and allows the Census Bureau to provide online self-service requests (e.g., subscriptions to publications, notifications, and partnerships) received through email, the web, or customer support lines.

(e) How information in the system is retrieved by the user

The subscriber will be able to access, retrieve, and update social media subscriptions on Decennial communications and/or advertisement platforms. All information is accessible via a web-based user interface where the user provides secure credentials.

Records maintained by this IT system are retrieved by email addresses and social media handles by authorized Census Bureau personnel only.

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

Transmission of HTTPS encryption happens at the boundary firewall. TLS encryption is utilized for connections to the IT system service offerings. All communications into and out of the

CEN37 services/components are also encrypted to provide FIPS 140-2 validated encryption. The encryption provides both confidentiality and integrity during transmission and reception.

(g) Any information sharing conducted by the system

ADCOM/CEN37 does not share any personally identifiable information (PII) or Title Data. However, analytical statistics data is captured and shared publicly as well as response rate data, which are retrieved from CEN18 Census Data Lake (CDL) System and personalization data retrieved from Adobe Target & Adobe Analytics. Neither response rates nor personalization data include PII. Lastly, Sprinklr and FaceBook Leads Generation applications collect user's trends and statistical data on these social media platforms.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. 301 and 44 U.S.C. 3101

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The 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.

__X__ 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):					

____ 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.

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
n. 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	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address*	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education*	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Social Media Handles					
*Advertisements in the Facebook Leads Generations application collect specific information that the user chooses to share with the Census Bureau. At a minimum this would include the user email address, however there may be times when an advertisement may ask for details about the educator; like names, subject, or grade level (all optional).					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History			
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

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

Government Sources					
Within the Bureau		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 Describe how the accuracy of the information in the system is ensured.

The Census Bureau relies on users to check their information for accuracy and timeliness when subscribing to CEN37 communications platforms. The information is provided directly by the subscriber, so it is up to the user to provide his/her email address accurately. Subscribers can change and/or verify their subscription information and preferences through their web-based subscriber preferences page.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		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	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): To improve communications between the Census Bureau and our subscribers.			

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 collection of PII is used to communicate to CEN37 stakeholders/subscribers so they can receive and stay up-to-date on information about Census Bureau programs and services. Anyone may subscribe; information is voluntary.

For web measurement and customization technologies, Tableau is a visualization tool to better understand statistical information. It takes in web statistics information from various external sources about how census.gov resources are used, and the results (No PII is posted) are published for review by stakeholders on an internal tableau server site.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention.

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Insider threats are not just malicious employees that intend to directly harm the company through theft or sabotage. Negligent employees unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees must complete mandatory security awareness training annually which includes Data Stewardship Awareness and Records Management training. In addition to the security protocols identified, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know. The information in the CEN37 is handled, retained and disposed of in accordance with appropriate record schedules.
CEN37 cloud encryption keys are maintained by the Census Bureau. The cloud provider will not have access to the encryption keys

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			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

X	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.

	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:
X	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 This system is a repository of information transferred from other systems. Notice is provided at the point of collection.	
	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.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Subscribers have the option to opt-out after reading the Privacy Act Statement. Users can also have their account removed at any time.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: It is an individual's choice whether to subscribe. If they desire this service, they must provide an email address, or the Census Bureau will not be able to send updates. If a subscriber no longer consents to how their PII is used, they can unsubscribe at any time. They will no longer receive services.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: Subscribers have the option to review their account profile and make updates. Customer Support is available, if help is needed.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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: Auditing the following: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☒ This is a new system/CEN Plan. 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 (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Census employees who are members of the support team will have access to the data in the IT system. All employees who will have access to the system are required to sign a confidentiality agreement/non-disclosure agreement/Code of Conduct that includes the requirement for confidentiality.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The 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 Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- 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 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(list all that apply)*: COMMERCE/DEPT-19- Mailing Lists- https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-19.html COMMERCE/DEPT-23- Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-23.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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: DAA -0029-2019-0004 : 2020 Decennial Record Schedule GRS 3.1, 3.2 and 6.4
	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	
Degaussing		Deleting	X
Other (specify):			

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

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. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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 PII itself is unlikely to result in harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII collected is required to be protected in accordance with: 5 U.S.C 301 and 44 U.S.C 3101
X	Access to and Location of PII	Provide explanation: The PII is physically located on servers owned and managed by a third-party vendor at offsite facilities located in the United States. The third-party vendors used are Federal Risk and Authorization Management Program (FedRAMP) approved Cloud Service Providers (CSPs).
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or

mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sworn employees who have an authorized business need to know.

12.2 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.

12.3 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.