Version Number: 01-2019

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

Privacy Threshold Analysis
for the
ASSOCIATE DIRECTOR FOR COMMUNICATIONS (ADCOM)

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/Associate Director for Communications (ADCOM)

Unique Project Identifier: [Number]

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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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

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. 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
   - 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 purpose that the system is designed to serve

The collection of PII/BII 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.

(e) The way the system operates to achieve the purpose

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.

(f) A general description of the type of information collected, maintained, use, or disseminated by the system

CEN37 ADCOM collects information such as name, email address, social media handles, etc… and 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.

(g) Identify individuals who have access to information on the system

U.S. Census Bureau employees and contractors have access to the CEN37 ADCOM systems.

(h) 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.

(i) 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.

Questionnaire:

1. What is the status of this information system?

_X_ 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). *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 01-2017 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. *(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_ National Institute of Standards and Technology Associates
_X_ Contractors working on behalf of DOC
_X_ Other Federal Government personnel
_X_ 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?

____ 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.

Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_ 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 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 CEN37 ADCOM 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 Information System Security Officer (ISSO): Renita L. Depp

Signature of ISSO: RENITA DEPP (Affiliate) Digitally signed by RENITA DEPP (Affiliate) Date: 2020.08.27 14:44:26 -04'00' Date: _____

System Owner (SO): Zachary H. Schwartz

Signature of SO: ZACHARY SCHWARTZ Digitally signed by ZACHARY SCHWARTZ Date: 2020.08.27 15:01:07 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Beau Houser

Signature of CISO: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2020.09.01 09:14:51 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.09.10 11:27:20 -04'00' Date: _____

Name of Technical Authorizing Official (TAO): Kevin Smith

Signature of AO: KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2020.09.03 11:12:59 -04'00' Date: _____

Name of Business Authorizing Official (BAO): Stephen L. Buckner

Signature of BAO: STEPHEN BUCKNER Digitally signed by STEPHEN BUCKNER Date: 2020.09.08 09:57:56 -04'00' Date: _____

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.09.10 11:27:39 -04'00' Date: _____