

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



**Privacy Threshold Analysis
for the
CEN09 Cloud Services**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau CEN09 Cloud Services

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

CEN09 is a general support system. The CEN09 Cloud Services general support system houses cloud based systems/components utilized by the U.S. Census Bureau. CEN09 can be described as the Census Bureau framework for cloud computing. Services/components in CEN09 spans multiple servers, and the physical environment is typically 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). These third-party cloud providers are responsible for keeping the data/information available and accessible, and the physical environment protected and running. Cloud services are bought or leased from the cloud provider, which transmits and stores user, organization, and application data.

(b) System location

AWS GovCloud is located in Oregon and Ohio

AWS East-1 is located in Virginia and East-2 is located in Ohio

AWS West-1 is located in California and West-2 is located in Oregon

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

CEN09 connects with/receives/maintains data from Census Bureau IT systems that are hosted on the CEN09 Infrastructure as a Service and Platform as a Service infrastructure/platforms.

(d) The purpose that the system is designed to serve

CEN09 is the Census Bureau framework for cloud computing. Services/components in CEN09 spans multiple servers, and the physical environment is typically owned and managed by a third-party vendor at offsite facilities located in the United States. These third-party cloud providers are responsible for keeping the data/information available and accessible, and the physical environment protected and running. Cloud services are bought or leased from the cloud provider, which transmits and stores user, organization, and application data.

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

The two current service models within CEN09 are:

- 1) Infrastructure as a Service (IaaS) – as defined by the NIST Special Publication 800-145 – the customer is provided processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

The following IaaS are authorized to operate in CEN09:

- a. AWS GovCloud (US) Region (GovCloud) is a logically isolated AWS Region located in the state of Oregon (OR) designed to allow US government agencies and contractors to move more sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. Customer applications are built upon the standard AWS services, and are considered outside of the system boundary. Customers are responsible for managing the security controls within their application.
- 2) Platform as a Service (PaaS) – as defined by the NIST Special Publication 800-145 – the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

The following PaaS is authorized to operate in CEN09:

- a. Amazon Web Services (AWS) GovCloud Platform as a Service (PaaS) model enables AWS to deliver hardware and software tools, needed for application development, to

its customers as a service. A PaaS provider hosts the hardware and software on its own infrastructure. As a result, the PaaS frees the customers from having to install in-house hardware and software to develop or run a new application. The Census Bureau currently offers managed shared web service that makes it easy to set up, operate, and scale databases in the cloud. These services are available for deployment with the AWS GovCloud infrastructure. The Census Bureau is responsible for providing standard deployment and configuration of the PaaS offerings. Tenant applications leveraging the PaaS offerings are outside of the authorization boundary.

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

The CEN09 Cloud Services stores and maintains Personally Identifiable Information (PII) /Business Identifiable Information (BII) for different program areas at the Census Bureau. Access to this data is only accessible by CEN09 on the administrative level.

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

U.S. Census Bureau employees and contractors

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

The CEN09 Cloud Services stores and maintains PII/BII for different program areas at the Census Bureau. CEN09 cloud service providers do not have access to the encryption keys of Census Bureau data so do not have access to the data.

CEN09 is not a system of records, therefore information is not retrieved at the PaaS and IaaS level by personal identifier.

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

Information is transmitted to and from CEN09 IaaS and PaaS cloud services only for authorized and lawful government purposes by employing secure communications with layered security controls including, but not limited to the use of validated FIPS 140-2 cryptographic modules and mechanisms to protect PII/BII.

Questionnaire:

1. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-Anonymous		e. New Public Access	h. Internal Flow or Collection
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): There has been a scope change for CEN09 to accommodate new hosts that utilize CEN09 IaaS and PaaS.			

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):	

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.

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."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

National Institute of Standards and Technology Associates

Contractors working on behalf of DOC

Other Federal Government personnel

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.

SSNs reside within IT systems, residing on CEN09 infrastructure. Individual IT system PIA's will contain SSN justifications.

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

SSN could reside within IT systems, residing on CEN09 infrastructure. Individual IT system PIA's will contain SSN justifications.

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?

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.

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

I certify the criteria implied by one or more of the questions above **apply** to CEN09 Cloud Services and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Kenneth Boyd

Signature of ISSO or SO: KENNETH BOYD Digitally signed by KENNETH BOYD Date: 2020.07.23 12:24:08 -04'00'

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

Signature of CISO: RONALD RINGGOLD Digitally signed by RONALD RINGGOLD Date: 2020.07.28 11:07:45 -04'00'

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.08.05 16:23:13 -04'00'

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO: KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2020.07.30 12:05:20 -04'00'

Name of Business Authorizing Official (AO): Gregg Bailey

Signature of AO: GREGG BAILEY Digitally signed by GREGG BAILEY Date: 2020.07.30 12:13:48 -04'00'

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2020.08.05 16:23:36 -04'00'