Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Office of the Chief Information Officer (OCIO) Cloud Services

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau Office of the Chief Information Officer (OCIO) 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: *Provide a brief description of the information system.*

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).

The OCIO Cloud Services general support system houses cloud-based systems/components utilized by the U.S. Census Bureau. This system can be described as the U.S. Census Bureau's framework for cloud computing. Services/components in OCIO Cloud Services 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) authorized 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.

The OCIO Cloud Services consists of IT systems supporting the U.S. Census Bureau's statistical mission of serving as the Nation's leading provider of quality data about its people and economy via the adoption of authorized FedRAMP cloud offerings under the shared-responsibility model. The current U.S. Census Bureau's enterprise cloud service catalog includes Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings with an expanding scope of services planned for future deployment.

Address the following elements:

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

OCIO Cloud Services is a general support system.

b) System location

Amazon Web Services GovCloud is located in Oregon and Ohio
Amazon Web Services East-1 is located in Virginia and East-2 is located in Ohio
Amazon Web Services West-1 is located in California and West-2 is located in Oregon
Microsoft Azure paired regions are located in Iowa and Virginia

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

OCIO Services connects with/receives/maintains data from U.S. Census Bureau's information systems that are hosted on the OCIO Cloud Services' Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

d) The purpose that the system is designed to serve

OCIO Cloud Services is the U.S. Census's Bureau framework for cloud computing. Services/components in this system span 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. OCIO 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 OCIO Cloud Services 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 OCIO Cloud Services:

a. Amazon Web Services GovCloud U.S. region is a logically isolated AWS Regions located in the states of Oregon and Ohio 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. Customer applications are built upon the standard AWS services, and are managed under their corresponding system boundary at the U.S. Census Bureau's Directorate level. Customers are responsible for managing the security controls within their application.

b. Amazon Web Services East/West located in U.S. East (Northern VA and Ohio) and U.S. West (Northern CA and Oregon) regions are utilized under the IaaS cloud computing model. The Amazon Web Services East/West IaaS enables convenient, on-demand Internet access to a shared pool of configurable Amazon Web Services computing resources such as servers, storage, network infrastructure, applications, and additional services. The U.S. Census Bureau is responsible for providing standard deployment and configuration of the IaaS offerings. Customer applications are built upon the standard AWS services, and are managed under their corresponding system boundary at the U.S. Census Bureau's Directorate level. 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 OCIO Cloud Services:

a. Amazon Web Services GovCloud logically isolated regions located in the states of Oregon and Ohio provide Platform as a Service (PaaS) 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 U.S. 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 U.S. Census Bureau is responsible for providing standard deployment and

configuration of the PaaS offerings. Tenant applications leveraging the PaaS offerings are managed under their corresponding system boundary at the U.S. Census Bureau's Directorate level.

b. Amazon Web Services located in U.S. East (Northern VA and Ohio) and U.S. West (Northern CA and Oregon) regions are utilized under the PaaS cloud computing service model. The Amazon Web Services Platform Service Management comprise managed web services that makes it easy to set up and operate services in the cloud. The U.S. Census Bureau creates instances and secure configurations that are uniform across the enterprise. The U.S. Census Bureau is responsible for providing standard deployment and configuration of the PaaS offerings. Customers are responsible for managing the security controls within their application and corresponding system boundary at the U.S. Census Bureau's Directorate level.

OCIO Cloud Services stores and maintains Personally Identifiable Information (PII)/Business Identifiable Information (BII) for different program areas at the U.S. Census Bureau. Access to this data is only accessible by OCIO Cloud Services on the administrative level. OCIO Cloud services IaaS and PaaS do not perform data dissemination however the IT systems hosted on OCIO Cloud Services may.

The following FedRAMP cloud-based technology offerings are currently within scope of the U.S. Census Bureau's agile authorization methodology for inclusion into the OCIO Cloud Services authorization to operate:

a. Microsoft Azure Commercial Cloud is an open and flexible cloud platform that enables customers to quickly build, test and deploy, and manage their applications, services, and product development across a network of Microsoft managed datacenters within the U.S. Microsoft Azure provides a multi-tenant public cloud services platform that offers functionality to support capacities such as Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) under FedRAMP shared-responsibility cloud computing models.

b. Microsoft Azure Government is a government-community cloud that offers hyper-scale compute, storage, networking, and identity management services, with world-class security. A physically and network-isolated instance of Microsoft Azure, operated by screened U.S. citizens, Azure Government provides standards-compliant IaaS and PaaS under the FedRAMP shared-responsibility cloud computing models.

OCIO Cloud services also plans to use a cloud service in FY23 to transcribe audio recordings for specific Demographic surveys. The recordings will be uploaded into the cloud, where a cloud

service will transcribe and analyze the recordings for a sponsored initiative by the Demographic area. The recordings will be removed within 30-90 days after the transcription is completed.

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

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

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

U.S. Census Bureau's employees and contractors

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

OCIO Cloud Services stores and maintains PII/BII for different program areas at the U.S. Census Bureau. Cloud Service's cloud providers do not have access to the encryption keys of U.S. Census Bureau's data, so they do not have access to the data.

Only authorized Census Bureau personnel has access to the data within OCIO Cloud Services. OCIO Cloud Services 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 OCIO Cloud Services 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. Status of the Information System

1a. What is the status of this information system?

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

__X__ 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	X	f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): There has been a scope change to OCIO Cloud Services with the inclusion of additional FedRAMP cloud services at the infrastructure level. Addition of audio recordings.					

____ 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. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X_ No. This is not a new information system.

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.

_X__ Yes. *(Check all that apply.)*

Activities			
Audio recordings	X	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.)."

__X__ 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."

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

_X___ DOC employees
_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?

_X___ 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.

SSN could reside in authorized information systems designed and deployed for such purpose within the U.S. Census Bureau's authorized FedRAMP boundary. 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 in authorized information systems designed and deployed for such purpose within the U.S. Census Bureau's authorized FedRAMP boundary. Individual IT system PIA's will contain SSN justifications and the applicable legal authorities.

____ 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 SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X___The criteria implied by one or more of the questions above **apply** to the Office of the Chief Information Officer (OCIO) Cloud Services and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the Office of the Chief Information Officer (OCIO) Cloud Services and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Gregg D. Bailey Office: Deputy Chief Information Officer Phone: 301-763-0989 Email: Gregg.D.Bailey@census.gov Signature: GREGG BAILEY Digitally signed by GREGG BAILEY Date: 2022.09.14 08:37:44 -04'00' Date signed:	**Chief Information Security Officer** Name: Beau Houser Office: Office of Information Security Phone: 301-763-1235 Email: beau.houser@census.gov Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2022.09.13 14:44:27 -04'00' Date signed:
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: Byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.09.15 16:28:30 -04'00' Date signed:	**Authorizing Official** Name: Luis J. Cano Office: Office of the Chief Information Officer Phone: (301) 763-3968 Email: luis.j.cano@census.gov Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2022.09.15 13:25:59 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: Byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.09.15 16:29:23 -04'00' Date signed:	