

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



**Privacy Threshold Analysis
for the
Cloud Research Environment (CRE)**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/ Cloud Research Environment (CRE)

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?

Cloud Research Environment (CRE) is a general support system that has major applications.

(b) System location

AWS Gov Cloud, Seattle, Washington

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

CRE interconnects with the CEN13 Integrated Research Environment (IRE). CRE and IRE are both within CEN13.

(d) The purpose the system is designed to serve

The purpose of this IT system is to provide a research environment in the commercial cloud for Census Bureau ADRM (Associate Directorate for Research and Methodology) researchers. The objective of the CRE is to provide a modern research computing environment to Census Bureau research users.

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

CRE provides infrastructure and software applications, as well as economic and demographic data to Census Bureau researchers so that they can perform research. Research users utilize

the data and software applications furnished to their project by the CRE to develop and execute research models to analyze and answer specific research questions related to their project.

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

This information maintained by CRE is obtained PII and BII from other Census Bureau program areas. Record linkage using BII and PIKs facilitates research to improve and support existing Census Bureau programs and creation of beta data products. These products use innovative techniques that leverage existing data and reduce the burden on respondents. This PII/BII covers members of the public, businesses, contractors and federal employees.

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

Government employees, contractors, and special sworn status employees of the Census Bureau.

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

The data files are stored on disk in various formats determined by the statistical software that they are to be processed with (SAS, Stata, R, etc.). Users use these statistical software packages to analyze the data. Data may also be stored in relational databases and retrieved through database queries. Retrieval of the data is performed only by authorized Census Bureau staff who have a need to know and are authorized through DMS.

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

Information is encrypted in accordance to Commerce requirements and sent using a virtual private network between CRE and other Census Bureau IT Systems. The VPN offers the required encryption. All data resides in Amazon Web Services (AWS) GovCloud (environment is specific only for Federal customers), and data is protected by disk level encryption and database encryption. In addition, the encryption keys are maintained by the Census Bureau. The cloud provider will not have access to the encryption keys.

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):			

- 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.

SSN's are often included in administrative record datasets that are acquired in support of the Census Bureau's title 13 authority to collect these data. When SSNs are present in these data they serve as one of several components used in a matching or look-up to assign an anonymized protected identification key (PIK) to the record.

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

Title 13, U.S.C. 6

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

X I certify the criteria implied by one or more of the questions above **apply** to the CEN13 CRE 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): Anup Mathur

Signature of SO: **ANUP MATHUR** Digitally signed by ANUP MATHUR Date: _____
Date: 2020.05.12 14:00:18 -04'00'

Name of Chief Information Security Officer: Beau Houser

Signature of CISO: **BEAU HOUSER** Digitally signed by BEAU HOUSER Date: _____
Date: 2020.06.03 14:19:12 -04'00'

Name of Privacy Act Officer (PAO): Byron Crenshaw

Signature of PAO: **BYRON CRENSHAW** Digitally signed by BYRON CRENSHAW Date: _____
Date: 2020.05.29 10:58:33 -04'00'

Name of Technical Authorizing Official (AO): Kevin Smith

Signature of AO: **KEVIN SMITH** Digitally signed by KEVIN SMITH Date: _____
Date: 2020.06.03 17:20:51 -04'00'

Name of Business Authorizing Official (AO): John Eltinge *Robert Sienkiewicz*

is Acting for John Eltinge and signs on his behalf.

Signature of AO: **ROBERT SIENKIEWICZ** Digitally signed by ROBERT SIENKIEWICZ Date: _____
Date: 2020.06.03 15:28:08 -04'00'

Name of Bureau Chief Privacy Officer (BCPO): Byron Crenshaw

Signature of BCPO: **BYRON CRENSHAW** Digitally signed by BYRON CRENSHAW Date: _____
Date: 2020.05.29 10:58:55 -04'00'