Template Version Number: 01-2021

U.S. Department of Commerce
Bureau of the Census

Privacy Threshold Analysis
for the
Associate Director for Research and Methodology (ADRM) Center for Optimization and Data Science (CODS)
Cloud Research Environment (CRE)

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau, Associate Director for Research and Methodology (ADRM) Center for Optimization and Data Science (CODS) 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: *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 Center for Optimization and Data Science (CODS) Cloud Research Environment (CRE) includes data maintained by the Census Bureau's Associate Director for Research and Methodology (ADRM). The CRE system is a cloud-based environment which allows researchers to work with data regarding research projects that support the Census Bureau mission. CRE provides an environment to use and leverage Census data that is stored within a cloud environment. The CRE solution produces a functional cloud environment hosted on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances that are securely configured provide users with a preconfigured solution environment for the analysis of large datasets. The information maintained by CRE is personally identifiable information (PII) and business identifiable information (BII) from other Census Bureau program areas. Record linkage using BII and PII 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 includes members of the public, businesses, contractors, and federal employees. To the maximum extent possible and consistent with the kind, timeliness, quality, and scope of the statistics required under Title 13 of the United States Code, the Census Bureau is required to obtain and use data from other agencies in lieu of direct inquiries through censuses or surveys.

Address the following elements:

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

Cloud Research Environment (CRE) is a general support system.

b) *System location*

AWS GovCloud Region US West (N. California)

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

CRE connects with the Integrated Research Environment (IRE). CRE and IRE are both within the Associate Directorate for Research and Methodology (ADRM).

d) *The purpose that 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 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 the 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, used, or disseminated by the system*

This information maintained by CRE is obtained PII/BII from other Census Bureau program areas. Record linkage using PII/BII 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 (statistical analysis system (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 the Data Management System (DMS).

i) How information is transmitted to and from the system

Information is encrypted in accordance with Commerce requirements and sent using a virtual private network (VPN) between CRE and other Census Bureau IT Systems. The VPN offers the required encryption. All data resides in 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. 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.*

____ 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.*

_X__ 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.

____ 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.)."

_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?

___ 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 SAOP 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 Cloud Research Environment (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.

System Owner Name: Robert Sienkiewicz Office: Center for Optimization and Data Science Phone: 301.763.1234 Email: robert.sienkiewicz@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ROBERT SIENKIEWICZ Digitally signed by ROBERT SIENKIEWICZ Date: 2022.12.05 15:35:02 -05'00' Date signed:	**Chief Information Security Officer** Name: Beau Houser Office: Office of Information Security Phone: 301.763.1235 Email: beau.houser@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2023.01.05 12:56:53 -05'00' Date signed:
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301.763.7997 Email: Byron.crenshaw@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.01.24 09:48:02 -05'00' Date signed:	**Authorizing Official** Name: Luis Cano Office: Office of the Chief Information Officer Phone: 301.763.3968 Email: luis.j.cano@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2023.01.05 14:47:13 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301.763.7997 Email: Byron.crenshaw@census.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.01.24 09:48:20 -05'00' Date signed:	**Business Authorizing Official** Name: John Eltinge Office: Office of the Associate Director for Research & Methodology Phone: 301.763.9604 Email: john.l.eltinge@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: JOHN ELTINGE Digitally signed by JOHN ELTINGE Date: 2023.01.10 11:48:56 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.