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) Computer Services Division (CSvD) Network Services

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/ OCIO CSvD Network 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).

OCIO Network Services consists of servers that are primarily managed by CSvD. A server is a computer or operating system that provides resources, data, services, or programs to other computers, known as clients, over a network. OCIO Network Services supports the Census Bureau's mission to collect United States (U.S.) statistical data. CSvD's mission is to provide the Census Bureau and other customers with a world-class computer center using state-of-the-art technology to monitor systems, communications, and applications.

In addition, the OCIO CSvD Network Services general support system hosts/contains the Census Bureau IT systems that may use, store, and maintain Personally Identifiable Information (PII)/Business Identifiable Information (BII) received from the public through surveys, censuses, or from other IT systems that use, store and maintain other PII including personnel data, etc. Access to this data is only accessible by OCIO CSvD Network Services server administrators.

OCIO CSvD Network Services does not perform dissemination of information; the IT systems hosted on OCIO Network Services servers perform information dissemination.

Address the following elements:

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

OCIO CSvD Network Services is a general support system

b) System location

The OCIO CSvD Network Services servers are located at the U.S. Census Bureau's Bowie Computer Center (BCC), Headquarters, and the Regional Offices.

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

OCIO CSvD Network Services connects with and hosts all Census Bureau IT systems that store and maintain information. Authentication information is received from OCIO Telecommunications Office (TCO) Data Communications IT systems.

d) The purpose that the system is designed to serve

To provide infrastructure capabilities for Census Bureau IT Systems.

e) The way the system operates to achieve the purpose

OCIO CSvD Network Services consists of servers that are primarily managed by the CSvD. The servers operate by hosting IT systems managed by other Census Bureau directorates. The PII/BII is maintained on OCIO CSvD Network Services server infrastructure for Storage Area Network (SAN) storage; data is not disseminated.

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

OCIO CSvD Network Services connects with/receives data from all Census Bureau IT systems. These IT systems may use, store, and maintain PII/BII received from the public through surveys, censuses, or from other IT systems that use, store and maintain other PII such as administrative and personnel data.

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

OCIO CSvD server administrators.

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

Information is not retrieved at the server level by personal identifier but may be retrieved by the hosted IT systems. Therefore, OCIO CSvD Network Services is not a Privacy Act system of records.

The information retrieved from IT systems containing PII/BII that are hosted on the OCIO CSvD Network Services servers are governed by the system of record notice(s) (SORN(s)) specific to the record types stored within the IT system and must be used in accordance with the purpose(s) identified in the SORN.

i) How information is transmitted to and from the system

No PII/BII is transmitted by the OCIO CSvD Network Services servers or operating system; only the IT systems hosted on the servers transmit information.

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?

__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. OCIO CSvD Network Services consists of servers that are primarily managed by the Computer Services Division (CSvD). The servers operate by hosting IT systems covered by other Census Bureau directorates. The PII/BII is maintained on OCIO CSvD Network Services server infrastructure for Storage Area Network (SAN) storage; data is not disseminated. Therefore, SSN could reside within IT systems, residing on OCIO CSvD Network Services server infrastructure. Other PIAs for IT systems hosted on OCIO CSvD Network Services servers will contain SSN justifications, as applicable.
Provide the legal authority which permits the collection of SSNs, including truncated form. Census Bureau IT systems that process PII/BII are hosted by OCIO CSvD Network Services servers. The legal authorities for those IT systems are listed on the individual PIAs applicable to those IT system boundaries.

____ 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 OCIO CSvD Network 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 OCIO CSvD Network Services and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer Name: Christopher Adams Office: Office of Information Security Phone: 202-875-2360 Email: christopher.adams@census.gov Signature: CHRISTOPHER ADAMS Digitally signed by CHRISTOPHER ADAMS Date: 2022.04.04 11:17:05 -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: 2022.04.12 09:31:37 -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: 2022.04.20 18:25:03 -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: 2022.04.15 08:49:47 -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: 2022.04.20 18:25:22 -04'00' Date signed:	