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) Client Support Division (CSD)

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau / Office of the Chief Information Officer (OCIO) Client Support Division (CSD)

Unique Project Identifier: 006-000401700

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:

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).

Office of the Chief Information Officer (OCIO) Client Support Division (CSD) is a general support system that supports Census Bureau employees by providing Enterprise IT support for desktop, laptop and printer services.

Address the following elements:

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

OCIO CSD is a general support system.

b) System location

OCIO CSD is located at the Bowie Computing Center.

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

OCIO CSD interconnects with other systems. The components of the OCIO CSD security plan share security tokens internally with the Office of the Chief Information Officer (OCIO) Telecommunications Office (TCO) Data Communications and the Office of the Chief

Information Officer (OCIO) Computer Services Division (CSvD) Network Services plan components. For example, an OCIO CSD component may request authentication of username, PIV, and Personal Identification Number (PIN) from a OCIO Data Communications component. OCIO CSD also connects with the Office of the Chief Information Officer (OCIO) Commerce Business System (CBS) to receive inventory control, account management, personal management and PII data from the OCIO CBS database. There is also a connection with the Office of the Chief Information Officer (OCIO) Human Resources applications to automate the exit process after an employee is terminated.

d) The purpose that the system is designed to serve

The purpose of the IT system is for administrative purposes. i.e., to assist in the management and maintenance of IT resources and for providing help desk assistance and end user services.

e) The way the system operates to achieve the purpose

A typical transaction on the components of OCIO CSD would be login and authentication to a desktop or virtual desktop using applications such as email, Microsoft Office products, web browsers, and databases. The authentication of customers to gain access to an IT system is processed externally to OCIO CSD (by connection to OCIO Data Communications).

In order for employees to use the desktops or virtual desktops, they must have a user ID, completed the data stewardship training, ad have received special sworn status (this status acknowledges that the individual has been sworn to protect information collected by the Census Bureau for life). In addition, a Personal Identity Verification (PIV) card is required. Secure ID is required for external access. PIV card is required for internal access.

The component used for managing cases is a tool that allows specially trained call center staff to capture the initial documentation of the issue. The issue is input, routed, and stored in the case management portion of the system that is carefully segregated from all other records. Only those with a need-to-know may access or view records.

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

The IT service management component documents and related any Census Bureau related IT problem and resolution. Pertinent information about the reported issue and any additional notes made are automatically time and date stamped. Employees, such as filed representatives or decennial enumerators, working from home rather than an office, have

their home as their duty station, thus their home address. Likewise, certain employees or contractors may have their personal email recorded as their business email address.

The sub-component that manages cases is used by several organizations within the Census Bureau. It is used for reporting, documenting, and resolving incidents. The data in the cases can include information about stolen or missing property, physical and IT security breaches, privacy incidents, and information related to any occupational safety cases.

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

U.S. Census Bureau employees and contractors including specially trained call center staff, Privacy Office staff, and Office of Information Security (OIS) staff.

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

In order for employees to use the desktops or virtual desktops, they must have a user ID, completed the data stewardship training, and have received special sworn status (this status acknowledges that the individual has been sworn to protect information collected by the Census Bureau for life). In addition, a Personal Identity (PIV) card is required. Secure ID is required for external access. PIV card is required for internal access.

Data is searchable by unique identifiers.

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

The components of OCIO CSD share security tokens internally with the OCIO Data Communications and the OCIO Network Services security plan components. For example, a OCIO CSD component may request authentication of username, PIV, and Personal Identification Number (PIN) from a OCIO Data Communications component. OCIO CSD component may then forward information of the authenticated element to a component within OCIO Network Services, such as providing an authenticated security token along with a request to access the data stored by that user name on the OCIO Network Services component. OCIO CSD shares information about the additional and retirement of hosts with Gov CloudForms, in the Network Services Boundary. This allows automatic updates of the assets. This information is transmitting using HTTPS. OCIO CSD has an interconnection agreement with the OCIO Human Resources application, Census Hiring and Employment Check (CHEC) system. This interconnection automates the exit process after a Census Bureau employee terminates employment. Data is transmitted via HTTPS.

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.

____ 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):			

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

____ 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.

__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) Client Support Division (CSD) Client 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) Client Support Division (CSD) Client Services and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer Name: Kwaku Afriyie Fordjour Office: Office of Information Security Phone: 301-763-7138 Email: kwaku.a.fordjour@census.gov Signature: KWAKU FORDJOUR (Affiliate) Digitally signed by KWAKU FORDJOUR (Affiliate) Date: 2023.05.22 11:40:56 -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: 2023.05.24 15:22:36 -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: 2023.05.25 14:58:34 -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: 2023.05.24 15:33:28 -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: 2023.05.25 14:58:47 -04'00' Date signed:	