Version Number: 01-2017

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

Privacy Threshold Analysis
for the
CEN17 Client Services

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/CEN17 Client Services

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 and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

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

CEN17 Client Services is a general support system.

b) System location

CEN 17 Client Services 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)

CEN17 Client Services interconnects with other systems. The components of the CEN17 Client Services security plan share security tokens internally with the CEN0 l Data Communications and the CEN16 Network Services security plan components. For example, a CEN l 7 component may request authentication of username, PIV, and Personal Identification Number (PIN) from a CEN0l component. The CEN17 component may then forward information of the authenticated element to a component within CEN16, such as providing an authenticated security token along with a request to access the data stored by that username on the CEN16 component. CEN17 also connects with CEN04 to receive inventory control, account management, personnel management and PII data from CEN04 CBS database. CEN17 also connects with CEN21to 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 CEN 17 Client Services 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 CEN l 7 (by connection to CENOl Data Communications).

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 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, use, or disseminated by the system

The IT service management component documents and describes 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 field representatives or decennial enumerators, working from their home rather than an office, have their home as their duty station, thus their home address is recorded as their business 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

Specially trained call center staff, Privacy Office, and Office of Information Security (OIS).

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 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 IT system that is carefully segregated from all other records. Only those with a need-to-know may access or view records.

i) How information is transmitted to and from the system

The components of the CEN17 Client Services security plan share security tokens internally with the CEN0l Data Communications and the CEN16 Network Services security plan components. For example, a CEN 1 7 component may request authentication of username, PIV, and Personal Identification Number (PIN) from a CEN0l component. The CEN17 component may then forward information of the authenticated element to a component within CEN16, such as providing an authenticated security token along with a request to access the data stored by that username on the CEN16 component. CEN17 shares information about the addition and retirement of hosts with CEN16 Gov CloudForms. This allows automatic updates of the assets. This information is transmitted using HTTPS. CEN17 has an interconnection agreement with CEN21 Census Hiring and Employment Check system. This interconnection automates the exit process after a Census Bureau employee terminates employment. Data is transmitted via HTTPS.

Questionnaire:

1. 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		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): New Interconnection					

____ 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 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. *Please describe the activities which may raise privacy concerns.*

_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.)."

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

____ Companies
____ Other business entities

_X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__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_ 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 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.

4c. 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, and/or 4c 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 CEN17 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): Patricia Trainor Musselman

Signature of SO: Patricia Musselman Date: 6-19-19

Name of Chief Information Security Officer (CISO): Jeffery W. Jackson

Signature of CISO: Jeffery W. Jackson Date: 26 Jun 2019

Name of Authorizing Official (AO): Kevin B. Smith

Signature of AO: Kevin Smith Date: 6-26-19

Name of Authorizing Official (AO): Gregg D. Bailey

Signature of AO: Gregg Bailey Date: 7/1/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw

Signature of BPO: Byron Crenshaw Date: 7/18/19