

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



**Privacy Threshold Analysis
for
CEN25 Office of Information Security (OIS)**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/CEN25 OIS

Unique Project Identifier: 006-000401500

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:

CEN25 collects, manages, and analyzes security information, event management data, logs, and other event data. This information is used to provide real-time alerting, forensic investigation, incident response, and compliance reporting. The information maintained within CEN25 components include: User ID, IP Addresses, and Date/Time of Access.

CEN25 integrates the System Security Plans (SSPs) and the risk assessment into a single, quantitative measure of risk to facilitate risk-based decisions.

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

Major applications

b) System location

Bowie Computer Center (BCC) and Suitland (HQ)

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

Interconnections for CEN25 are restricted to audit log data from all Census Bureau servers, network devices, and storage solutions.

d) The purpose that the system is designed to serve

The Office of Information Security interprets information security requirements and standards, educates Census staff on information security, facilitates and validates implementation of information security requirements and standards, and reports on information security compliance on behalf of the agency.

e) The way the system operates to achieve the purpose

CEN25 has a number of systems that help aggregate audit logs, alert on malicious traffic or actions, document system security plans for Bureau-wide information systems, conduct vulnerability and compliance scans, and process forensic data to help with security investigations.

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

The PII is collected in reference to federal employees and contractors that use Census Bureau Systems. User ID's, JBID's, IP Addresses, and Date and Time of Access are collected for cyber security purposes including log analysis, intrusion detection, and vulnerability scanning.

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

Information is restricted to OIS personnel contingent to the jobs they perform.

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

Each tool has a specified console to retrieve information. The access is restricted to only approved personnel.

i) How information is transmitted to and from the system

Information is only collected from the Census Bureau end points. Servers, network devices, storage have to be configured to send syslog data to the audit log aggregator.

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.*

 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 (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.*

_____ 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

☐ 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..."

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

☐ DOC employees

☐ Contractors working on behalf of DOC

☐ 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?

☐ 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.
- _____ 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 the CEN25 OIS 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 CEN25 OIS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): William Bradd _____

Signature of SO:  Date: 5/1/18

Name of Chief Information Security Officer (CISO): Timothy Ruland _____

Signature of CISO:  Date: 5/3/18

Name of Authorizing Official (AO): Kevin Smith _____

Signature of AO:  Date: 5/14/18

Name of Bureau Privacy Officer (BPO): Byron Crenshaw _____

Signature of BPO:  Date: 5/15/18