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

Privacy Threshold Analysis
for the
CEN31 Administrative Systems Vol. II
U.S. Department of Commerce Privacy Threshold Analysis
U.S. Census Bureau/CEN31 Administrative Systems Vol. II

Unique Project Identifier: 006-000403600

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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:

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

CEN31, Administrative Systems Vol. II, encompasses the wide variety of Administrative Business Solutions within Administrative & Customer Services Division (ACSD), Associate Director for Field Regional Offices (ADF/ROs), Office of Congressional & Intergovernmental Affairs (OCIA), and Policy Coordination Office (PCO).

CEN31 includes the following applications or components:

- CENdocS (Census Document System) which is the web-based system for requesting 1) Forms design services, 2) Publications and graphics services, and 3) Printing services. It is integrated with the CBS system.
- Records Control Database Application which tracks the location of physical records.
- Conference Reservation System (EMS Pro / Virtual EMS) professional application is used to manage reservations for the first floor conference rooms, training rooms, and the auditorium. Access is available to all census employees using the web interface.
- WorldShare Management System Online Computer Library Center [or Ohio College Library Center] Software as a Service (WMS OCLC SaaS): WorldShare gives people the ability to view library collections from anywhere in the world. The library staff is the primary user of the Library Management System for checking in and checking out books.
- Environmental Monitoring System (Avtech) is a software/hardware solution to monitor the temperature/ humidity in the HQ Data Centers.
- Enterprise Mail Metering System (Connect+, SendSuite Live) is a collection of mail metering stations located at Census headquarters, the 6 regional offices, and the National
Processing Center that are used to place postage on outgoing United States Postal Service (USPS) mail pieces or parcels. The transactions are recorded and later imported into the CBS Postal System.

- Correspondence Oversight & Tracking System (COTS) [Entellitrak by Tyler Technologies] is a valuable tool used to route and manage permanent record correspondence between the Director's office and Program Areas within the Census Bureau.

(b) System location

CEN31 applications are hosted at Census Bureau Headquarters, except for WMS OCLC SaaS which is located at their HQ in Dublin, OH & their data center in Waterville, OH.

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

CEN31 has an established interconnection with CEN04, Commerce Business Systems (CBS) which provides some of the PII needed for eligibility to services covered by CEN31. CEN31 also interconnects with CEN01, CEN16, and CEN18 for authentication/infrastructure purposes.

(d) The purpose that the system is designed to serve

The PII collected by the applications covered by CEN31 are used to identify users, authorize users, and control to applications.

(e) The way the system operates to achieve the purpose(s)

CEN31 applications are used throughout the U.S. Census Bureau in accomplishing its mission in an efficient manner. The program areas’ business solutions provide timely, relevant, high-quality products and services, and ensure a productive and safe work environment to support the U.S. Census Bureau and its employees in meeting and exceeding the Agency's mission, strategic goals and objectives.

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

CEN31 maintains very little PII. The PII maintained within CEN31 is name, employee id, work email address, work address, and work phone number.

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

U.S. Census Bureau government employees and contractors have access to CEN31.

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

CEN31 information can be retrieved by an identifier such as name or employee id. Information contained in the CEN31 information systems are available to authorized U.S. Census Bureau
federal employees and contractors.

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

Information is transmitted between CEN31 and Census Bureau enterprise systems. CEN31 components use enterprise supported SQL Server and Oracle databases. CEN31 also uses enterprise support LDAP services for user authentication. These connections are all encrypted. CEN31 components also receives software updates from external vendors using the HTTPS encrypted protocol. There's an additional connection with a vendor, PitneyBowes, where electronic funds are downloaded to our postal meters. This connection is also encrypted as required by the United States Postal Service.
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.

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
</tr>
</tbody>
</table>

   _____ 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).  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 01-2017 or later).  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.)

<table>
<thead>
<tr>
<th>Activities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
<td></td>
</tr>
<tr>
<td>Building entry readers</td>
<td></td>
</tr>
<tr>
<td>Video surveillance</td>
<td></td>
</tr>
<tr>
<td>Electronic purchase transactions</td>
<td></td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
</tr>
</tbody>
</table>

_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.__

_X_ 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

___ National Institute of Standards and Technology Associates

_X_ 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.

___ 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 approved PIA must be a part of the IT system’s Assessment and Authorization Package.
CERTIFICATION

I certify the criteria implied by one or more of the questions above apply to the CEN31 Administrative Systems Vol. II 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): David J. Peters
Signature of SO: DAVID PETERS Date: 2021.01.28 13:15:31 -05'00' Date: ___________

Name of Chief Information Security Officer (CISO): Beau Houser
Signature of CISO: BEAU HOUSER Date: 2021.01.28 17:07:27 -05'00' Date: ___________

Name of Authorizing Official (AO): Gregg D. Bailey
Signature of AO: GREGG BAILEY Date: 2021.01.29 10:18:43 -05'00' Date: ___________

Name of Authorizing Official (AO): Laura K. Furgione
Signature of AO: LAURA FURGIONE Date: 2021.01.29 12:50:04 -05'00' Date: ___________

Name of Bureau Privacy Officer (BPO): Byron Crenshaw
Signature of BPO: BYRON CRENSHAW Date: 2021.02.11 17:42:58 -05'00' Date: ___________

Name of Privacy Act Officer (PAO): Byron Crenshaw
Signature of PAO: BYRON CRENSHAW Date: 2021.02.11 17:43:20 -05'00' Date: ___________