

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



**Privacy Threshold Analysis**  
**for the**  
**CEN02 Lenel System**

## U.S. Department of Commerce Privacy Threshold Analysis

### U.S. Census Bureau CEN02 Lenel

**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 (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*

The CEN02 Lenel IT system is an electronic access control system that controls physical access via HSPD-12 (Homeland Security Presidential Directive 12) compliant PIV (Personal Identification Verification) card access. The IT system reads the employee badges for facility access, equipment access, and appropriate identification. It grants access to various physical environments and defines employee access levels.

*(b) System location*

CEN02 Lenel is housed at the Census Bureau’s Bowie, MD computer center

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

CEN02 Lenel interconnects with infrastructure services at the U.S. Census Bureau. This includes CEN01 for authentication/telecommunication purposes, CEN16 for server/storage, and CEN17 for laptops and workstations.

*(d) The purpose that the system is designed to sever*

The CEN02 Lenel administrative system supports the day-to-day administrative functions, physical access to facilities and some specific security functions

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

The Department of Commerce Office of Security at the Census Bureau utilizes CEN02 Lenel to monitor and track user access. The IT system also includes video surveillance capabilities at all Census Bureau facilities. The Lenel system is maintained and supported by a contractor, SightComm, STARS II Partnership Joint Venture LLC (replaced Communications Resource, Inc. (CRI) in FY2015). The IT system is accessed from a limited number of workstations located at the Census Bureau headquarters in Suitland, MD, and a limited workstation located at the Jeffersonville, IN, OSY Field Office. Each of the six Census Bureau field offices has one workstation dedicated for the Lenel system.

A typical transaction on the IT system is to allow or deny an employee facility access and equipment access via an encoded employee badge which shows appropriate identification. All Census Bureau personnel are issued Federal HSPD-12 Personal Identification Verification (PIV) cards. The user's information is entered into a back-end user database that can be updated to reflect changes in employee status or access permissions. The card readers are connected to access control appliances connected to the IT system via the Census Bureau Local Area Network (LAN), and access the user database to determine whether users are permitted to enter the restricted area that they are attempting to access.

The IT system provides information about various alarms. It will display the date, time, location, and provide additional information pertaining to the priority level of the alarm. In addition, it provides specific details about the asset or cardholder's name that triggered the alarm while tracking and locating the cardholder. The IT system has the ability to alert administrators of an alarm event through automatic alphanumeric pages or e-mail messages during the event.

An automatic cardholder call-up feature allows for quick search and display of images in the database which holds picture identification, employee credentials, and employee accesses. The IT system includes card readers integrated with electronic door locks, elevator programming, card encoders, and a user database. All Census Bureau personnel are issued ID badges that are embedded with Radio Frequency-Identification technology (RFID) tags. The user's information is entered into a back-end user database that can be updated to reflect changes in employee status or access permissions. The card readers are all connected to the IT system via hardwired connections to access management appliances connected to the Census Bureau Local Area Network (LAN), and access the user database to determine whether users are permitted to enter the restricted area that they are attempting to access.

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

CEN02 Lenel pulls name, user id, and employee ID from an employee's PIV card. CEN02 Lenel also collects the users work email address and work phone number in addition to dates and times of access to the U.S. Census Bureau for each employee. Video Surveillance is performed for security status monitoring and investigations on federal employees/contractors, members of public, foreign nationals or visitors.

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

Authorized U.S. Census Bureau employees and contractors have access to CEN02 Lenel

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

Authorized CEN02 Lenel system users can retrieve information by name, user id, and employee id.

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

Reports are shared on a case-by-case basis and include very little PII (name and user id) along with corresponding PIV badge scan-in and scan-out times and locations. If a report needs to be shared, they are shared securely via email.

**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.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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 01-2017). *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 01-2019 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.)

Activities			
Audio recordings		Building entry readers	X
Video surveillance	X	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.

☒ 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   I certify the criteria implied by one or more of the questions above **apply** to the CEN02 Lenel 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.

<p><b>Information System Security Officer or System Owner</b>  Name: Robert J. Drew  Office: Chief Administration Office  Phone: 301-763-8340  Email: robert.j.drew@census.gov</p> <p style="text-align: right;">Digitally signed by ROBERT DREW JR. Date: 2020.12.15 17:22:47 -05'00'</p> <p>Signature: <u>ROBERT DREW JR.</u></p> <p>Date signed: _____</p>	<p><b>Chief Information Security Officer</b>  Name: Beau Houser  Office: Chief, Office of Information Security  Phone: 301-763-1235  Email: beau.houser@census.gov</p> <p style="text-align: right;">Digitally signed by RONALD RINGGOLD Date: 2020.12.22 10:13:34 -05'00'</p> <p>Signature: <u>RONALD RINGGOLD</u></p> <p>Date signed: _____</p>
<p><b>Privacy Act Officer</b>  Name: Byron Crenshaw  Office: Policy Coordination Office (PCO)  Phone: 301-763-7997  Email: byron.crenshaw@census.gov</p> <p style="text-align: right;">Digitally signed by BYRON CRENSHAW Date: 2021.01.12 11:43:58 -05'00'</p> <p>Signature: <u>BYRON CRENSHAW</u></p> <p>Date signed: _____</p>	<p><b>Technical Authorizing Official</b>  Name: Kevin B. Smith  Office: Associate Director of IT &amp; CIO  Phone: 301-763-2117  Email: kevin.b.smith@census.gov</p> <p style="text-align: right;">Digitally signed by KEVIN SMITH Date: 2020.12.22 15:21:48 -05'00'</p> <p>Signature: <u>KEVIN SMITH</u></p> <p>Date signed: _____</p>
<p><b>Bureau Chief Privacy Officer</b>  Name: Byron Crenshaw  Office: Policy Coordination Office (PCO)  Phone: 301-763-7997  Email: byron.crenshaw@census.gov</p> <p style="text-align: right;">Digitally signed by BYRON CRENSHAW Date: 2021.01.12 11:44:21 -05'00'</p> <p>Signature: <u>BYRON CRENSHAW</u></p> <p>Date signed: _____</p>	<p><b>Business Authorizing Official</b>  Name: Laura K Furgione  Office: Chief Administrative Officer  Phone: 301-763-0264  Email: laura.furgione@census.gov</p> <p style="text-align: right;">Digitally signed by LAURA FURGIONE Date: 2020.12.23 07:59:27 -05'00'</p> <p>Signature: <u>LAURA FURGIONE</u></p> <p>Date signed: _____</p>