

**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:**

- a) *Whether it is a general support system, major application, or other type of system*
- b) *System location*
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) *The purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from the system*

The CEN02 Lenel 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 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. The IT system is housed at the Census Bureau's Bowie, MD computer center.

The 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 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 system includes card readers integrated with electronic door locks, elevator programming, card encoders, and a user database. All Census 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 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.

The Office of Security at Census utilizes the system to monitor and track user access. The system also includes video surveillance capabilities for the Census premises. The system is maintained and supported by a contractor, SightComm, STARS II Partnership Joint Venture LLC (replaced Communications Resource, Inc. (CRI) in FY2015). The system is accessed from a limited number of workstations located at the Census 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 system.

The Lenel IT system interconnects with the Census IT infrastructure system for the Enterprise ID Management System (IDMS). Users logging on to the Lenel system are authenticated at the network level using their network managed IDMS credentials when they connect to the Lenel application. Data within Lenel regarding physical badge numbers, card status and user names is also synched with the IDMS.

**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.*

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. Building entry readers. Video surveillance.

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 PIA 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 CEN02 Level 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 CEN02 Level and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Owner (SO): Robert Drew (Acting)  
Office: Department of Commerce, Office of Security

Signature of ISSO or SO: Robert Drew Date: 7-9-19

Name of Chief Information Security Officer (CISO): Jeffrey Jackson  
Office: Chief Information Security Officer (CISO) (Acting)

Signature of CISO: Jeffrey Jackson Date: 7/9/19

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

Signature of AO: Kevin B. Smith Date: 7/9/19

Name of Authorizing Official (AO): David R. Ziaya  
Office: Office of the Director

Signature of AO: David R. Ziaya Date: 7/9/19

Name of Bureau Privacy Officer (BPO): Byron Crenshaw  
Office: Policy Coordination Office (PCO)

Signature of BCPO: Byron Crenshaw Date: 7/9/19