Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Office of the Chief Administrative Officer (OCAO) Lenel

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau Chief Administrative Office (OCAO) 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: *Provide a brief description of the information system.*

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).

The LENEL system provides the Census with a method of controlling employee and contractor access to secure areas. The system includes card readers integrated with electronic door locks and elevator programming, card encoders, a user database, and video monitoring capabilities. All Census personnel are issued ID badges that are embedded with Radio Frequency Identification (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 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 LENEL system to monitor and track user accesses. The system also includes video surveillance capabilities for the Census premises. The LENEL system is maintained and supported by a contractor, Communications Resource, Inc. (CRI). The LENEL system is accessed from a limited number of workstations located at the Census headquarters in Suitland, MD, and limited workstation located at the Jeffersonville, IN, Office of Security (OSY) Field Office. Each of the twelve field offices has one workstation dedicated for the LENEL system.

Address the following elements:

a) Whether it is a general support system, major application, or other type of system

The 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

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)

Lenel interconnects with infrastructure services at the U.S. Census Bureau. This includes Office of the Chief Information Officer (OCIO) Data Communications for authentication/telecommunication purposes, OCIO Network Services for server/storage, and OCIO Client Services for laptops and workstations.

d) The purpose that the system is designed to serve

The 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

The Department of Commerce Office of Security at the Census Bureau utilizes 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

Lenel pulls name, user id, and employee ID from an employee's PIV card. 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 Lenel

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

Authorized 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.*

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. *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.

_X_ 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.

_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
_X_ Contractors working on behalf of DOC
_X_ Other Federal Government personnel

_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 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 SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☑ The criteria implied by one or more of the questions above **apply** to OCAO Lenel and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the SharePoint and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Robert J. Drew Office: Office of the Chief Administrative Officer Phone: 301-763-8340 Email: robert.j.drew@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ROBERT DREW JR. Digitally signed by ROBERT DREW JR. Date: 2022.03.15 15:59:22 -04'00' Date signed:	**Chief Information Security Officer** Name: Beau Houser Office: Office of the Chief Information Officer Phone: 301-763-1235 Email: beau.houser@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2022.03.16 10:44:47 -04'00' Date signed:
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: byron.crenshaw@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.03.21 10:55:48 -04'00' Date signed:	**Authorizing Official** Name: Luis J. Cano Office: Office of the Chief Information Officer Phone: (301) 763-3968 Email: luis.j.cano@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2022.03.17 09:33:26 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301-763-7997 Email: byron.crenshaw@census.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.03.21 10:56:06 -04'00' Date signed:	**Authorizing Official** Name: Laura K Furgione Office: Office of the Chief Administrative Officer Phone: 301-763-0264 Email: laura.furgione@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: VERONICA LEGRANDE Digitally signed by VERONICA LEGRANDE Date: 2022.03.17 10:52:59 -04'00' Date signed: