Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Office of the Chief Administrative Office (OCAO) Office of Security (OSY) LENEL

Reviewed by: Byron Crenshaw, Bureau Chief Privacy Officer

(●) Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
( ) Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

BYRON CRENSHAW Digitally signed by BYRON CRENSHAW
Date: 2023.03.07 11:42:02 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/ Office of the Chief Administrative Office (OCAO) OSY LENEL

Unique Project Identifier: 006-000401700

Introduction: System Description

Provide a brief description of the information system.

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 six 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 OCAO 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 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 way the system operates to achieve the purpose(s) identified in Section 4

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 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 LAN and access the user database to determine whether users are permitted to enter the restricted area that they are attempting to access.

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

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

(f) 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.

(g) Any information sharing

Data may be shared only on a case-by-case bases for investigative purposes.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-		e. New Public Access		h. Internal Flow or	

Anonymous				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.

__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.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): user id also known as James bond id (Jbid)					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance			

		Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos	X	k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

PII (Name, employee id, and user id) for each user in Lenel is pulled from the user's PIV badge. Administrators then use Lenel to grant appropriate physical and equipment access. Accuracy of access is ensured via an approval process in Remedy Case Management System (OCIO Client Services), where the approval goes through a chain of approvers, including the employee's supervisors.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Physical access to facilities			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

For Administrative Matters and Physical Access to facilities:

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

- Employee ID is collected from employees and contractors. The employee number (Commerce Business System first identifier) and James Bond ID (JBID second identifier) are required for data exchange between Department of Commerce (DOC) and the Census Bureau access control system.
- Name is collected from employees and contractors; it is required for identification purposes.
- Telephone Number (work & cell phone) is collected about employees and contractors, it is required for emergency management purposes (work number)
- Email Address is collected from employees, it is a third identifier for data base update.
- Photographs of federal employees/contractors, members of public, foreign nationals or visitors. are collected and required for ID purposes
- User ID/Badge PIV Number is collected from employees. It is required for access control and is encoded on the ID cards issued to employees.
- Date/Time of access is collected from federal employees/contractors, members of public, foreign nationals or visitors when individuals enter or exit the Census Bureau facilities. This is also collected for emergency management situations.
- Video Surveillance is performed for security status monitoring and investigations on federal employees/contractors, members of public, foreign nationals or visitors.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The census Bureau also deploys a Data Loss Prevention solution.

The information in Lenel is handled, retained and disposed of in accordance with appropriate federal record schedules.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Lenel systems interconnects with infrastructure services at the U.S. Census Bureau. This includes OCIO Data Communications for authentication/telecommunication purposes, OCIO Network Services for server/storage, and OCIO Client Services for laptops and workstations. The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following: • Intrusion Detection | Prevention Systems (IDS | IPS) • Firewalls • Mandatory use of HTTP(S) for Census Bureau Public facing websites • Use of trusted internet connection (TIC) • Anti-Virus software to protect host/end user systems • Encryption of databases (Data at rest) • HSPD-12 Compliant PIV cards • Access Controls The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system

	within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The census Bureau also deploys a Data Loss Prevention solution.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.census.gov/about/policies/privacy/privacy-policy.html	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The user does not have the ability to decline PII/BII for the Lenel system as information is used to produce PIV cards that grant physical access to the building and are required under HSPD-12.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The user does not have the ability to consent to particular uses of PII/BII for the Lenel system as information is used to produce PIV cards that grant physical access to the building and are required under HSPD-12

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals are able to review/update information within the appropriate Census Bureau applications. In addition, individuals may review/update information by Privacy Act Request and Freedom of Information Act (FOIA) Request for video surveillance.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition, audit logs are in place and assessed per NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 07/13/2022 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention (DLP) solution/tool as well.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X_ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/Dept-25, Access Control and Identity Management System: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: IRS Pub 1075; Visitor Access Logs Section 4.3.1
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Combined data elements uniquely and directly identify individuals.
X	Quantity of PII	Provide explanation: A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, or the PII itself may result in serious harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide requirements. Violations may result in serious civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. PII is not stored or transported off-site by employees or contractors.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of

information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

System Owner
Name: Robert J. Drew
Office: Office of the Chief Administration 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: 2023.01.24 12:11:23 -05'00'

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: 2023.02.21 08:22:46 -05'00'

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: 2023.03.07 11:42:56 -05'00'

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: 2023.02.23 10:17:58 -05'00'

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: 2023.03.07 11:43:29 -05'00'

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.